

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS ACF2 STIG

Version: 6

Release: 43

29 Dec 2020

XSL Release 5/15/2012 Sort by: STIGID
Description:

Group ID (Vulid): V-82
Group Title: AAMV0010

Rule ID: SV-82r2_rule

Severity: CAT III

Rule Version (STIG-ID): [AAMV0010](#)

Rule Title: A CMP (Change Management Process) is not being utilized on this system.

Vulnerability Discussion: Without proper tracking of changes to the operating system software environment, its processing integrity and availability are subject to compromise.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECSD-1, ECSD-2

Check Content:

a) Generate a list of SMP/E CSI data sets using ISPF 3.4

1. From ISPF 3.4 enter Dsname Level *.*.CSI

b) Execute the following sample JCL to generate a listing of installed products and features

```
//STEP1 EXEC PGM=GIMSMP,REGION=0M
//SYSPRINT DD SYSOUT=*
//SMPOUT DD SYSOUT=*
//SMPCSI DD DISP=SHR,DSN= << CSI DATA SET
//SMPLIST DD DSN=YOURHLQ.FEATURE.LIST,
// DCB=(RECFM=FBA,LRECL=121,BLKSIZE=12100),
// SPACE=(CYL,(1,1,)),
// DISP=(NEW,CATLG)
//SMPCNTL DD *
SET BDY(GLOBAL) /* SET TO GLOBAL ZONE. */.
LIST FEATURE.
/*
/*-----*
/* ADD STEPS AS REQUIRED FOR ALL ADDITIONAL CSI DATA SETS
/* REPORTS WILL BE APPENDED TO THE FEATURE LIST
/*-+---1---+---2---+---3---+---4---+---5---+---6---+---7*
//STEP2 EXEC PGM=GIMSMP
//SYSPRINT DD SYSOUT=*
//SMPOUT DD SYSOUT=*
//SMPCSI DD DISP=SHR,DSN=ANOTHER.GLOBAL.CSI << ADDITIONAL CSI
//SMPLIST DD DSN=YOURHLQ.FEATURE.LIST,
```

```
// DISP=MOD
//SMPCNTL DD *
SET BDY(GLOBAL) /* SET TO GLOBAL ZONE. */.
LIST FEATURE.
/*
```

NOTE 1: SMP/E CSIs may not be present on this domain. If the site uses another domain to install products via SMP/E, and then copies the SMP/E product installation libraries to this domain, this is acceptable.

Review the domain where the SMP/E environment resides and compare it against the domain being reviewed for compliance.

The Z/OS STIG states that all products with the capability for installation via IBM s SMP/E process will be installed and maintained using that process.

c) If the entries contained in the SMP/E CSIs accurately reflect the operating system software environment, there is NO FINDING.

d) If the entries contained in the SMP/E CSIs do not accurately reflect the operating system software environment, this is a FINDING.

Fix Text: The systems programmer responsible for supporting changes to the software will ensure that all changes and updates are tracked and maintained using a CMP. Obtain/locate all applicable SMP/E data sets (e.g., CSI, PTS, etc.). Ensure that all entries contained in the SMP/E configuration are matched with the operating system environment. Verify with the Systems programmer that the components of the operating system are controlled through a CMP.

Note: Many systems are created from a base system that is controlled by a change management program. Be sure to note that the system has been maintained based on this process.

CCI: CCI-000326

Group ID (Vulid): V-7545

Group Title: AAMV0012

Rule ID: SV-8016r3_rule

Severity: CAT I

Rule Version (STIG-ID): [AAMV0012](#)

Rule Title: Unsupported system software is installed and active on the system.

Vulnerability Discussion: When a vendor drops support of System Software, they no longer maintain security vulnerability patches to the software. Without vulnerability patches, it is impossible to verify that the system does not contain code which could violate the integrity of the operating system environment.

Responsibility: N/A

IAControls: N/A

Check Content:

a) Refer to the list of supported software products found in the SS0 Supported Software Version Release Table in the z/OS STIG Addendum.

b) If the software products currently running on the reviewed system are at a version greater than or equal to the products listed in the z/OS STIG Addendum, there is NO FINDING.

c) If the software products currently running on the reviewed system are at a version less than the products listed in the z/OS STIG Addendum or additional products are APF authorized or access sensitive data, then this is a finding.

Fix Text: For all products that meet the following criteria:

- Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries.
- Require access to system datasets or sensitive information or requires special or privileged authority to run.

The ISSO will ensure that unsupported system software for the products in the above category is removed or upgraded prior to a vendor dropping support.

Authorized software which is NO longer supported is a CAT I vulnerability. The customer and site will be given 6 months to mitigate the risk, come up with a supported solution or obtain a formal letter approving such risk/software.

CCI: CCI-001764

CCI: CCI-001765

Group ID (Vulid): V-7546

Group Title: AAMV0014

Rule ID: SV-8019r3_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0014](#)

Rule Title: Site must have a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support.

Vulnerability Discussion: Vendors' code may contain vulnerabilities that may be exploited to cause denial of service or to violate the integrity of the system or

data on the System. Most vendors develop patches to correct these vulnerabilities. When vendors' products become unsupported, the creation of these patches cease leaving the system exposed to any future vulnerabilities not patched. Without a documented migration plan established to monitor system software versions and releases unsupported software may be allowed to run on the system.

Responsibility: Security Manager

IAControls: N/A

Check Content:

- a) Check with the Systems programmer to make sure that documented procedures exist to monitor the software products in SS0 Supported Software Version Release Table in the z/OS STIG Addendum. to verify dates it will become unsupported and to notify management to start procedures to upgrade to supported versions of the products before that date.
- b) If documented procedures exist to monitor products in SS0 Supported Software Version Release Table in the z/OS STIG Addendum for dates they will become unsupported and to notify management to upgrade to supported versions of the products this is not a finding.
- c) If documented procedures do not exist to monitor products in SS0 Supported Software Version Release Table in the z/OS STIG Addendum for dates they will become unsupported and to notify management to upgrade to supported versions of the products this is a finding.

Note: If product support is provided through an outside group, verify that they have a process to notify site of unsupported software.

Fix Text: The ISSO/ISSM will verify that a process is documented and followed for unsupported software.

CCI: CCI-000409

CCI: CCI-001225

CCI: CCI-001227

CCI: CCI-002606

CCI: CCI-002615

CCI: CCI-002617

Group ID (Vulid): V-15209

Group Title: AAMV0018

Rule ID: SV-15984r2_rule

Severity: CAT I

Rule Version (STIG-ID): [AAMV0018](#)

Rule Title: Site does not maintain documented procedures to apply security related software patches to their system and does not maintain a log of when these patches were applied.

Vulnerability Discussion: Vendors' code may contain vulnerabilities that may be exploited to cause denial of service or to violate the integrity of the system or data on the System. Most vendors develop patches to correct these vulnerabilities. These patches must be applied and documented.

Responsibility: Information Assurance Officer

IAControls: DCAR-1, DCCS-1, DCCS-2

Check Content:

- a) Check with the Information Assurance Officer to make sure that documented procedures exist for security related software patches to be scheduled, applied and documented.
- b) If the documented procedures exist to monitor, apply and document software patches than this is not a finding.
- c) If the documented procedures do not exist to monitor, apply and document software patches than this is a finding.

Fix Text: The IAO will ensure that all security related software patches are scheduled to be applied and documented.

System Programmers and IAOs should regularly check OS vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be scheduled to be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site s responsibility to test vendor patches within their test environment.

CCI: CCI-001220

CCI: CCI-002605

Group ID (Vulid): V-83

Group Title: AAMV0030

Rule ID: SV-83r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0030](#)

Rule Title: LNKAUTH=APFTAB is not specified in the IEASYSxx member(s) in the currently active parmlib data set(s).

Vulnerability Discussion: Failure to specify LINKAUTH=APFTAB allows libraries other than those designated as APF to contain authorized modules which could bypass security and violate the integrity of the operating system environment. This expanded authorization list inhibits the ability to control inclusion of these modules.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

- a) From Analyzer main Menu, go to 3;L;<ENTER>
- b) Place a B next to the first occurrence of IEASYSnn
- d) If LNKAUTH=APFTAB is specified, there is NO FINDING.
- e) If LNKAUTH=APFTAB is NOT specified, this is a FINDING.

Fix Text: The systems programmer will ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) in the currently active parmlib data set(s). Review all installed software for authorization requirements. Identify and include only libraries with this requirement in the APF designation. Change LINKAUTH=LNKLST to LINKAUTH=APFTAB in all IEASYSxx members.

Control over APF authorization is specified within the operating system. The data set SYS1.PARMLIB members IEAAPFxx and PROGxx are used to specify the library names and the volumes on which they reside. (The xx is the suffix designated by the APF and PROG parameters in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at system initial program load [IPL]).

NOTE: An entire library is listed as authorized, and not the individual modules themselves.

Use the following recommendations and techniques to control the exposures created by the APF facility:

- (1) In SYS1.PARMLIB(IEASYSxx), use the parameter LNKAUTH=APFTAB so that all APF libraries are specified in the IEAAPFxx and PROGxx members of parmlib.

CCI: CCI-000381

CCI: CCI-001762

CCI: CCI-002283

Group ID (Vulid): V-84

Group Title: AAMV0040

Rule ID: SV-84r2_rule

Severity: CAT III

Rule Version (STIG-ID): [AAMV0040](#)

Rule Title: Inaccessible APF libraries defined.

Vulnerability Discussion: If a library designated by an APF entry does not exist on the volume specified, a library of the same name may be placed on this volume and inherit APF authorization. This could allow the introduction of modules which bypass security and violate the integrity of the operating system environment.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

- a) From Analyzer main Menu, go to 4;B. Specify S next to APF table in the upper half of the screen. Specify YES for Exceptions Only and NO for all other options on the lower half of the screen. Submit the batch job and reference the report output.
- b) If there are no entries in the report with finding messages, there is NO FINDING for inaccessible APF Libraries.
- c) If there are entries in the report with finding messages, there is a FINDING for inaccessible APF libraries.

Fix Text: The systems programmer will ensure that only existing libraries are specified in the APF list of libraries. Review the entire list of APF authorized libraries and remove those which are no longer valid designations.

(2) The IEAAPFxx members will contain only required libraries. On a semi annual basis, Software Support should review the volume serial numbers, and should verify them in accordance with the system catalog. Software Support will remove all non existent libraries. The IAO should modify and/or delete the rules associated with these libraries.

CCI: CCI-000381

CCI: CCI-001762

CCI: CCI-002283

Group ID (Vulid): V-85

Group Title: AAMV0050

Rule ID: SV-85r2_rule

Severity: CAT III

Rule Version (STIG-ID): [AAMV0050](#)

Rule Title: Duplicated sensitive utilities and/or programs exist in APF libraries.

Vulnerability Discussion: Modules designated as sensitive utilities have the ability to significantly modify the operating system environment. Duplication of these modules causes an exposure by making it extremely difficult to track modifications to them. This could allow for the execution of invalid or trojan horse versions of these utilities.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) From Analyzer main Menu, go to 4;B. Specify S next to APF tables in the upper half of the screen. Specify YES for Duplicate Module Analysis and NO for all other options on the lower half of the screen. Submit the batch job and reference the report output. Review the Duplicate Module Analysis section of the report.

b) If duplicate APF modules exist, compare the duplicates to the modules specified below:

1.The following list contains Sensitive Utilities that will be checked.

AHLGTF

AMASPZAP
AMAZAP
AMDIOCP
AMZIOCP
BLSROPTR
CSQJU003
CSQJU004
CSQUCVX
CSQUTIL
CSQ1LOGP
DEBE
DITTO
FDRZAPOP
GIMSMP
HHLGTF
ICKDSF
ICPIOCP
IDCSC01
IEHINITT
IFASMFD
IGWSPZAP
IHLGTF
IMASPZAP
IND\$FILE
IOPIOCP
IXPIOCP
IYPIOCP
IZPIOCP
WHOIS
L052INIT
TMSCOPY
TMSFORMT
TMSLBLPR
TMSMULV
TMSREMOV
TMSTPNIT
TMSUDSNB

c) If none of the sensitive utilities are duplicated, there is NO FINDING.

d) If any of the sensitive utilities are duplicated, this is a FINDING.

Fix Text: The IAO will ensure that duplicate sensitive utility(ies) and/or program(s) do not exist in APF-authorized libraries. Identify all versions of the sensitive utilities contained in APF-authorized libraries listed in the above check. In cases where duplicates exist, ensure no exposure has been created and written justification has been filed with the IAO.

(3) Before a library and a volume serial number are added to IEAAPFxx and PROGxx, the IAO will protect the data set from unauthorized access. Systems programming personnel will specify the requirements for users needing read or execute access to this library. Comparisons among all the APF libraries will be done to ensure that an exposure is not created by the existence of identically named modules. Address any sensitive utility concerns with the IAO, so that the function can be restricted as required. The IAO will build the appropriate protection into the ACP.

CCI: CCI-001762

CCI: CCI-002283

Group ID (Vulid): V-86

Group Title: AAMV0060

Rule ID: SV-86r3_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0060](#)

Rule Title: The review of AC=1 modules in APF authorized libraries will be reviewed annually and documentation verifying the modules integrity is available.

Vulnerability Discussion: The review of AC=1 modules that reside in APF authorized libraries will be reviewed annually. The IAO will maintain documentation identifying the integrity and justification of Vendor APF authorized libraries. For non-vendor APF authorized libraries, the source and documentation identifying the integrity and justification that describes the AC=1 module process will be maintained by the IAO. Sites have undocumented and/or unauthorized AC=1 modules have a possible risk to the confidentiality, integrity, and availability of the system and present a clear risk to the operating system, ACP, and customer data.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

Verify that AC=1 modules identified in the APF Authorized data sets specified in EXAM.RPT(APFXRPT) have documentation and/or source code. If the following guidance is true, this is not a finding.

___ Documentation for Vendor APF Authorized libraries identifying the integrity and justification are maintained by the IAO.

___ Documentation and source code for non-vendor AC=1 modules in APF Authorized libraries identifying the integrity and justification are maintained by the IAO.

___ Review of all Vendor and non-vendor AC=1 modules in APF Authorized libraries will be reviewed on an annual basis.

Fix Text: The IAO working with the systems programmer will ensure that documentation and/or source code are available for AC=1 modules that reside in the APF Authorized libraries.

Documentation for Vendor APF Authorized libraries identifying the integrity and justification will be available. Examples of this type of documentation can be in the form of product installation guides or product system programming guides.

Documentation and source code for non-vendor AC=1 modules in APF Authorized libraries identifying the integrity and justification will be available.

A review of the above documentation and/or source will be performed on an annual basis.

CCI: CCI-000643

CCI: CCI-001829

CCI: CCI-002736

Group ID (Vulid): V-90

Group Title: AAMV0160

Rule ID: SV-90r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0160](#)

Rule Title: Inapplicable PPT entries have not been invalidated.

Vulnerability Discussion: If invalid or inapplicable PPT entries exist, a venue is provided for the introduction of trojan horse modules with security bypass capabilities.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

a) From Analyzer main Menu, go to 4;A. Specify YES for Perform Module Search, YES for Exceptions Only, and NO for Sort Criteria. Submit the batch job and reference the report output.

b) Review report for any entries with message VSA334R .

1. If any of the entries in the report that have message VSA334R associated with them have any of the following settings, then there is a FINDING:

- a. Bypass password protection: Yes
- b. No Dataset Integrity? Yes
- c. Protect Key (if required): 00-07

2. If ALL of the entries in the report that have message VSA334R associated with them DO NOT have any of the following settings, then there is NO FINDING:

- a. Bypass password protection: Yes
- b. No Dataset Integrity? Yes
- c. Protect Key (if required): 00-07

Fix Text: The systems programmer will ensure that any invalid entries in the PPT via IEFSDPPT module or invalid entries in the SCHED PPT are nullified by (a) nullifying the invalid IEFSDPPT entry ensuring that there is a corresponding SCHED entry which confers no special attributes, or (b) removing the SCHED PPT entry which is no longer valid if it only exists in this member.

Review the PPT and ensure that all entries associated with non-existent or inapplicable modules are invalidated. As applicable, either: (a) nullify the invalid IEFSDPPT entry by ensuring that there is a corresponding SCHED entry which confers no special attributes, or (b) remove the SCHED PPT entry which is no longer valid.

Some programs require extraordinary privileges not normally permitted by the operating system. The Program Properties Table (PPT) contains the names and properties of these special programs. Programs in the PPT can bypass security software mechanisms such as password protection. Only programs that require special authorizations are coded in the PPT.

The PPT is maintained differently depending upon the level of MVS. Use the following recommendations and techniques to provide protection for the PPT:

- (1) As part of standard MVS maintenance, systems programming personnel will review the IEFSDPPT module and all programs that IBM has, by default, placed in the PPT to validate their applicability to the execution system. Please refer to the IBM z/OS MVS Initialization and Tuning Reference documentation for the version and release of z/OS installed at the individual site for the actual contents of the default IEFSDPPT
- (2) Modules for products not in use on the system will have their special privileges explicitly revoked. Do this by placing a PPT entry for each module in the

SYS1.PARMLIB(SCHEDxx) member, specifying no special privileges. The PPT entry for each overridden program will be in the following format, accepting the default (unprivileged) values for the sub parameters:

PPT PGMNAME(<program name>)

(3) The Software Support team will assemble documentation regarding these PPT entries, and the IAO will keep it on file. Include the following in the documentation:

- The product and release for which the PPT entry was made
- The last date this entry was reviewed to authenticate status
- The reason the module's privileges are being revoked

CCI: CCI-000381

Group ID (Vulid): V-5605

Group Title: AAMV0325

Rule ID: SV-5605r2_rule

Severity: CAT III

Rule Version (STIG-ID): [AAMV0325](#)

Rule Title: Non-existent or inaccessible Link Pack Area (LPA) libraries.

Vulnerability Discussion: LPA libraries give a common access point for the general usage of modules. Many of the subsystems installed on a domain rely upon these modules for proper execution. If the list of libraries found in this LPA member is not properly maintained, the integrity of the operating environment is subject to compromise.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

- From Analyzer main Menu, go to 4;B. Specify S next to LPA List table in the upper half of the screen. Specify YES for Exceptions Only and NO for all other options on the lower half of the screen. Submit the batch job and reference the report output.
- If there are no entries in the report with finding messages, there is NO FINDING for inaccessible LPA List Libraries.

c) If there are entries in the report with finding messages, there is a FINDING for inaccessible LPA List libraries.

Fix Text: The systems programmer will ensure that only existing libraries are specified in the LPA list of libraries.

Review all entries contained in the LPA members for the actual existence of each library. Develop a plan of action to correct deficiencies.

The system Link Pack Area (LPA) is the component of MVS that maintains core operating system functions resident in main storage. A security concern exists when libraries from which LPA modules are obtained require APF authorization.

Control over residence in the LPA is specified within the operating system in the following members of the data set SYS1.PARMLIB:

- LPALSTxx specifies the names of libraries to be concatenated to SYS1.LPALIB when the LPA is generated at IPL in an MVS/XA or MVS/ESA system. (The xx is the suffix designated by the LPA parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at system initial program load [IPL].)
- IEAFIXxx specifies the names of modules from SYS1.SVCLIB, the LPALSTxx concatenation, and the LNKLSTxx concatenation that are to be temporarily fixed in central storage in the Fixed LPA (FLPA) for the duration of an IPL. (The xx is the suffix designated by the FIX parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at IPL.)
- IEALPAXx specifies the names of modules that will be loaded from the following:
 - ? SYS1.SVCLIB
 - ? The LPALSTxx concatenation
 - ? The LNKLSTxx concatenation as a temporary extension to the existing Pageable

LPA (PLPA) in the Modified LPA (MLPA) for the duration of an IPL. (The xx is the suffix designated by the MLPA parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at IPL.)

Use the following recommendations and techniques to control the exposures created by the LPA facility:

- (1) The LPALSTxx, IEAFIXxx, and IEALPAXx members will contain only required libraries. On a semi annual basis, Software Support should review the volume serial numbers, and should verify them in accordance with the system catalog. Software Support will remove all non existent libraries. The IAO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001762

CCI: CCI-001764

Group ID (Vulid): V-100

Group Title: AAMV0350

Rule ID: SV-100r2_rule

Severity: CAT III

Rule Version (STIG-ID): [AAMV0350](#)

Rule Title: Non-existent or inaccessible LINKLIST libraries.

Vulnerability Discussion: LINKLIST libraries give a common access point for the general usage of modules. Many of the subsystems installed on a domain rely upon these modules for proper execution. If the list of libraries found in this LINKLIST is not properly maintained, the integrity of the operating environment is subject to compromise.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) From Analyzer main Menu, go to 4;B. Specify S next to Link List Table (All libraries) in the upper half of the screen. Specify YES for Exceptions Only and NO for all other options on the lower half of the screen. Submit the batch job and reference the report output.

b) If there are no entries in the report with finding messages, there is NO FINDING for inaccessible LINKLIST Libraries.

c) If there are entries in the report with finding messages, there is a FINDING for inaccessible LINKLIST libraries.

Fix Text: The systems programmer will ensure that only existing libraries are specified in the Linklist list of libraries.

Review all entries contained in the LINKLIST for the actual existence of each library. Develop a plan of action to correct deficiencies.

The Linklist is a default set of libraries that MVS searches for a specified program. This facility is used so that a user does not have to know the library names in which utility types of programs are stored. Control over membership in the Linklist is specified within the operating system. The data set SYS1.PARMLIB(LNKLISTxx) is used to specify the library names. (The xx is the suffix designated by the LNK parameter in the IEASYSxx member of SYS1.PARMLIB, or overridden by the computer operator at IPL.)

Use the following recommendations and techniques to control the exposures created by the LINKLIST facility:

- (1) Avoid inclusion of sensitive libraries in the LNKLSTxx member unless absolutely required.
- (2) The LNKLSTxx and PROGxx (LNKLST entries) members will contain only required libraries. On a semi annual basis, Software Support should review the volume serial numbers, and should verify them in accordance with the system catalog. Software Support will remove all non existent libraries. The IAO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001762

CCI: CCI-001764

Group ID (Vulid): V-101

Group Title: AAMV0370

Rule ID: SV-101r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0370](#)

Rule Title: Non-standard SMF data collection options specified.

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit trails from each of the ACPs. If the control options for the recording of this tracking are not properly maintained, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3

Check Content:

- a) From Analyzer main Menu, go to 3;L;<ENTER>
- b) Place a B next to the first occurrence of SMFPRMnn
- c) If all the options for SMF data gathering are set as required (in the table shown at the end of this STIG) there is NO FINDING.

NOTE: Issues with subtype 4 and 5 of type 30 records can be exempted from collection. The following is an example of the entry to perform this:

SUBSYS(STC,EXITS(IEFU29,IEFU83,IEFU84,IEFUJP,IEFUSO),
INTERVAL(SMF,SYNC),NODETAIL)

NOTE: If the JWT parameter is greater than 15 minutes, and the system is processing unclassified information, review the following items. If any of these items is true, there is NO FINDING.

d) If a session is not terminated, but instead is locked out after 15 minutes of Inactivity, a process must be in place that requires user identification and Authentication before the session is unlocked. Session lock-out will be Implemented through system controls or terminal screen protections.

e) A system s default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.

f) The IAM may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:

The time-out exception cannot exceed 60 minutes.

A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site IAM. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).

The requirement must be revalidated on an annual basis.

If variances from the below SMF collection options (with the exception of the ones mentioned in (b) above), this is a FINDING.

The settings for several parameters are critical to the collection process:

ACTIVE: Activates the collection of SMF data.

JWT(15): The maximum amount of consecutive time that an

executing job may spend as ineligible to use any CPU resources before being canceled for inactivity. The STIG requirement for Job Wait Time is 15 minutes. (This may be extended if controlled through other means, e.g., a Session Manager or ACP.)

MAXDORM(0500): Specifies the amount of real time that SMF allows data to remain in an SMF buffer before it is written to a recording data set.

SID: Specifies the system ID to be recorded in all SMF records.

SYS(DETAIL): Controls the level of detail recorded.

SYS(INTERVAL): Ensures the periodic recording of data for long running jobs.

SYS: Specifies the types and sub types of SMF records that are to be collected.

SYS(TYPE) indicates that the supplied list is inclusive (i.e., specifies the record types to be collected). Record types not listed are not collected.

SYS(NOTYPE) indicates that the supplied list is exclusive (i.e., specifies those record types not to be collected). Record types not listed are not collected. The site may use either form of this parameter to specify SMF record type collection. However, at a minimum all record types listed.

Fix Text: The IAO will ensure that collection options for SMF Data are consistent with options specified below.

Review all SMF recording specifications found in SMFPRMxx members. Ensure that SMF recording options used are consistent with those outlined below.

The settings for several parameters are critical to the collection process:

ACTIVE Activates the collection of SMF data.

JWT(15) The maximum amount of consecutive time that an executing job may spend as ineligible to use any CPU resources before being canceled for inactivity. The requirement for Job Wait Time is 15 minutes. (This may be extended if controlled through other means, e.g., a Session Manager or ACP.)

NOTE: The JWT parameter can be greater than 15 minutes if the system is processing unclassified information and the following items are reviewed.

- 1) If a session is not terminated, but instead is locked out after 15 minutes of inactivity, a process must be in place that requires user identification and authentication before the session is unlocked. Session lock-out will be implemented through system controls or terminal screen protections.
- 2) A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM or IAO. The IAM and/or IAO will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.
- 3) The IAM and/or IAO may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:
 - (a) The time-out exception cannot exceed 60 minutes.
 - (b) A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site IAM or IAO. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).
 - (c) The requirement must be revalidated on an annual basis.

MAXDORM(0500) Specifies the amount of real time that SMF allows data to remain in an SMF buffer before it is written to a recording data set.

SID Specifies the system ID to be recorded in all SMF records

SYS(DETAIL) Controls the level of detail recorded.

SYS(INTERVAL) Ensures the periodic recording of data for long running jobs.

SYS Specifies the types and sub types of SMF records that are to be collected. SYS(TYPE) indicates that the supplied list is inclusive (i.e., specifies the record types to be collected). Record types not listed are not collected. SYS(NOTYPE) indicates that the supplied list is exclusive (i.e., specifies those record types not to be collected). Record types not listed are not collected. The site may use either form of this parameter to specify SMF record type collection. However, at a minimum all record types listed.

CCI: CCI-000057

CCI: CCI-000130

CCI: CCI-001844

CCI: CCI-001851

Group ID (Vulid): V-102

Group Title: AAMV0380

Rule ID: SV-102r4_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0380](#)

Rule Title: Required SMF data record types must be collected.

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit records from each of the ACPs and system. If the required SMF data record types are not being collected, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2

Check Content:

a) From Analyzer main Menu, go to 4;H. Specify YES next to Record Type cross-reference and NO for all other options. Submit the batch job and reference the report output. Review the Record Type Cross-reference section of the report.

b) If all of the required SMF record types (as specified below in the table IBM SMF RECORDS TO BE COLLECTED AT A MINIMUM) are being collected, there is NO FINDING.

c) If any of the required record types is not being collected, this is a FINDING.
IBM SMF RECORDS TO BE COLLECTED AT A MINIMUM

0 (00) IPL

6 (06) External Writer/ JES Output Writer/ Print Services Facility (PSF)

7 (07) [SMF] Data Lost

14 (0E) INPUT or RDBACK Data Set Activity

15 (0F) OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity

17 (11) Scratch Data Set Status

18 (12) Rename Non-VSAM Data Set Status

24 (18) JES2 Spool Offload

25 (19) JES3 Device Allocation

26 (1A) JES Job Purge

- 30 (1E) Common Address Space Work
- 32 (20) TSO/E User Work Accounting
- 41 (29) DIV Objects and VLF Statistics
- 42 (2A) DFSMS statistics and configuration
- 43 (2B) JES Start
- 45 (2D) JES Withdrawal/Stop
- 47 (2F) JES SIGNON/Start Line (BSC)/LOGON
- 48 (30) JES SIGNOFF/Stop Line (BSC)/LOGOFF
- 49 (31) JES Integrity
- 52 (34) JES2 LOGON/Start Line (SNA)
- 53 (35) JES2 LOGOFF/Stop Line (SNA)
- 54 (36) JES2 Integrity (SNA)
- 55 (37) JES2 Network SIGNON
- 56 (38) JES2 Network Integrity
- 57 (39) JES2 Network SYSOUT Transmission
- 58 (3A) JES2 Network SIGNOFF
- 60 (3C) VSAM Volume Data Set Updated
- 61 (3D) Integrated Catalog Facility Define Activity
- 62 (3E) VSAM Component or Cluster Opened
- 64 (40) VSAM Component or Cluster Status
- 65 (41) Integrated Catalog Facility Delete Activity
- 66 (42) Integrated Catalog Facility Alter Activity
- 80 (50) RACF/TOP SECRET Processing
- 81 (51) RACF Initialization
- 83 (53) RACF Audit Record For Data Sets
- 90 (5A) System Status
- 92 (5C) except subtypes 10, 11 OpenMVS File System Activity
- 102 (66) DATABASE 2 Performance
- 103 (67) IBM HTTP Server
- 110 (6E) CICS/ESA Statistics
- 118 (76) TCP/IP Statistics
- 119 (77) TCP/IP Statistics
- 199 (C7) TSOMON
- 230 (E6) ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
- 231 (E7) TSS logs security events under this record type

Fix Text: The IAO and systems programming personnel will ensure that SMF recording options are consistent with those outlined below.

IBM SMF Records to be collect at a minimum

| | |
|----------|---|
| 0 (00) | IPL |
| 6 (06) | External Writer/ JES Output Writer/ Print Services Facility (PSF) |
| 7 (07) | [SMF] Data Lost |
| 14 (0E) | INPUT or RDBACK Data Set Activity |
| 15 (0F) | OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity |
| 17 (11) | Scratch Data Set Status |
| 18 (12) | Rename Non-VSAM Data Set Status |
| 24 (18) | JES2 Spool Offload |
| 25 (19) | JES3 Device Allocation |
| 26 (1A) | JES Job Purge |
| 30 (1E) | Common Address Space Work |
| 32 (20) | TSO/E User Work Accounting |
| 41 (29) | DIV Objects and VLF Statistics |
| 42 (2A) | DFSMS statistics and configuration |
| 43 (2B) | JES Start |
| 45 (2D) | JES Withdrawal/Stop |
| 47 (2F) | JES SIGNON/Start Line (BSC)/LOGON |
| 48 (30) | JES SIGNOFF/Stop Line (BSC)/LOGOFF |
| 49 (31) | JES Integrity |
| 52 (34) | JES2 LOGON/Start Line (SNA) |
| 53 (35) | JES2 LOGOFF/Stop Line (SNA) |
| 54 (36) | JES2 Integrity (SNA) |
| 55 (37) | JES2 Network SIGNON |
| 56 (38) | JES2 Network Integrity |
| 57 (39) | JES2 Network SYSOUT Transmission |
| 58 (3A) | JES2 Network SIGNOFF |
| 60 (3C) | VSAM Volume Data Set Updated |
| 61 (3D) | Integrated Catalog Facility Define Activity |
| 62 (3E) | VSAM Component or Cluster Opened |
| 64 (40) | VSAM Component or Cluster Status |
| 65 (41) | Integrated Catalog Facility Delete Activity |
| 66 (42) | Integrated Catalog Facility Alter Activity |
| 80 (50) | RACF/TOP SECRET Processing |
| 81 (51) | RACF Initialization |
| 83 (53) | RACF Audit Record For Data Sets |
| 90 (5A) | System Status |
| 92 (5C) | except subtypes 10, 11 OpenMVS File System Activity |
| 102 (66) | DATABASE 2 Performance |
| 103 (67) | IBM HTTP Server |
| 110 (6E) | CICS/ESA Statistics |

118 (76) TCP/IP Statistics
119 (77) TCP/IP Statistics
199 (C7) TSOMON
230 (E6) ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
231 (E7) TSS logs security events under this record type

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000169

CCI: CCI-000172

CCI: CCI-001353

CCI: CCI-001487

Group ID (Vulid): V-103
Group Title: AAMV0400
Rule ID: SV-103r2_rule
Severity: CAT II

Rule Version (STIG-ID): [AAMV0400](#)

Rule Title: An automated process is not in place to collect and retain SMF data.

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data is the audit trail from the ACP. If the control options for the recording of this tracking are not properly maintained, then accountability cannot be monitored and its use in the execution of a contingency plan could be compromised. Failure to collect SMF data in a timely fashion can result in the loss of critical system data.

Responsibility: Information Assurance Officer

IAControls: CODB-2, DCCS-1, DCCS-2

Check Content:

a) Refer to Vulnerability Questions within the SRRAUDIT Dialog Management document.

1. Ensure all documents are current and being followed.

b) Ensure at least the following are covered in the documents.

1. Retain at least two (2) copies of the SMF data

2. Maintain SMF data for a minimum of one year

3. All update and alter access authority to SMF history files will be logged using the ACP's facilities. Only systems programming personnel and batch jobs that perform SMF functions will be authorized to update the SMF files. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

c) If, based on the information provided, it can be determined that an automated process is in place to collect and retain all SMF data produced on the system, and all items in section b are being adhered to, there is NO FINDING

d) If it cannot be determined this process exists and is being adhered to, or that any one item in section b is not followed, this is a FINDING.

Fix Text: The IAO will ensure that an automated process is in place to collect SMF data.

Review SMF data collection and retention processes. Ensure that the processes utilized include a process which is automatically started to dump SMF collection files immediately upon their becoming full.

To ensure that all SMF data is collected in a timely manner, and to reduce the risk of data loss, the site will ensure that automated mechanisms are in place to collect and retain all SMF data produced on the system. Dump the SMF files (MANx) in systems based on the following guidelines:

(a) Dump each SMF file as it fills up during the normal course of daily processing.

(b) Dump all remaining SMF data at the end of each processing day.

CCI: CCI-001348

CCI: CCI-001353

Group ID (Valid): V-104

Group Title: AAMV0410

Rule ID: SV-104r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0410](#)

Rule Title: ACP database is not on a separate physical volume from its backup and recovery datasets.

Vulnerability Discussion: The ACP backup and recovery data files provide the only means of recovering the ACP database in the event of its damage. In the case where this damage is to the physical volume on which it resides, and any of these recovery data files exist on this volume as well, then complete recovery of the ACP database would be extremely difficult, if even possible.

Responsibility: Systems Programmer

IAControls: CODB-2, DCCS-1, DCCS-2

Check Content:

) Refer to the following item gathered from the z/OS Data Collection:

- Step 8 (c)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(AAMV0410)

For RACF sites only, refer to the following report produced by the RACF Data Collection:

- DSMON.RPT(RACDST)

For ACF2 sites only, refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFBKUP)

For TSS sites only, refer to the following report produced by the z/OS Data Collection, review procedure library member TSS for information:

- EXAM.RPT(PROCLIBS)

b) If the Access Control Product (ACP) database is not located on the same volume as either its alternate or backup file, there is NO FINDING.

Fix Text: The systems programmer will ensure that placement of ACP files are on a separate volume from its backup and recovery data sets to provide backup and recovery in the event of physical damage to a volume.

Identify the ACP database(s), backup database(s), and recovery data set(s). Develop a plan to keep these data sets on different physical volumes. Implement the movement of these critical ACP files.

File location is an often overlooked factor in system integrity. It is important to ensure that the effects of hardware failures on system integrity and availability are minimized. Avoid collocation of files such as primary and alternate databases. For example, the loss of the physical volume containing the ACP database should not also cause the loss of the ACP backup database as a result of their collocation. Files that will be segregated from each other on separate physical volumes include, but are not limited to, the ACP database and its alternate or backup file.

CCI: CCI-000549

Group ID (Vulid): V-105

Group Title: AAMV0420

Rule ID: SV-105r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0420](#)

Rule Title: ACP database is not backed up on a scheduled basis.

Vulnerability Discussion: Loss of the ACP database would cause an interruption in the service of the operating system environment. If regularly scheduled backups of this database are not processed, system recovery time could be unacceptably long.

Responsibility: Information Assurance Officer

IAControls: CODB-2, DCCS-1, DCCS-2

Check Content:

a) Check with the IAO and verify that procedures exist to backup the security data base and files. Have the IAO identify the dataset names and frequency of the backups.

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(AAMV0420)

For ACF2 sites only, refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFBKUP)

For TOP SECRET sites only, refer to the following report produced by the TOP SECRET Data Collection:

- TSSCMDS.RPT(STATUS)

Note: RACF creates an alternate data set and does not have any setting to specify that a backup is created

b) If, based on the information provided, it ca

Fix Text: The IAO will ensure that procedures are in place to backup all ACP files needed for recovery on a scheduled basis.

Identify the ACP database and ensure that documented processes are in place to back up its contents on a regularly scheduled basis.

At a minimum, nightly backup of the ACP databases, and of other critical security files (such as the ACP parameter file). More frequent backups (two or three times daily) will reduce the time necessary to affect recovery. The IAO will verify that the backup job(s) run successfully.

CCI: CCI-000537

Group ID (Vulid): V-106

Group Title: AAMV0430

Rule ID: SV-106r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0430](#)

Rule Title: System DASD backups are not performed on a regularly scheduled basis.

Vulnerability Discussion: If backups of the operating environment are not properly processed, implementation of a contingency plan would not include the data necessary to fully recover from any outage.

Responsibility: Information Assurance Officer

IAControls: CODB-2, DCCS-1, DCCS-2

Check Content:

Refer to Vulnerability Questions within the SRRAUDIT Dialog Management document.

a) If, based on the information provided, it can be determined that system DASD backups are performed a regularly scheduled basis, there is NO FINDING.

b) If it cannot be determined that system DASD backups are performed on a regularly scheduled basis, this is a FINDING.

Fix Text: The IAO will ensure that procedures are in place to backup the operating system and all its subsystems on a regularly scheduled interval as required to recover the environment.

Review all documented processes for the backup of the operating environment. Ensure that these include a regularly scheduled backup of the entire operating system and its related subsystems, both at individual data set and full volume levels.

Adequate backup scheduling is also an often overlooked integrity exposure. Back up system files on a regular schedule. Store the backups off site to prevent concurrent loss of the live production system and the backup files. Backup scheduling will vary depending on the requirements and capabilities of the individual data center.

While the requirements of Data Owners may necessitate more frequent backups, a recommended schedule is as follows:

- Weekly and monthly full volume backup of volumes with low update activity, such as the operating system volumes
- Nightly backup of high update activity data sets and volumes, such as application system databases and user data volumes

CCI: CCI-000537

Group ID (Vulid): V-107

Group Title: AAMV0440

Rule ID: SV-107r2_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0440](#)

Rule Title: PASSWORD data set and OS passwords are utilized.

Vulnerability Discussion: All protection of system resources must come from the ACP. If multiple protection mechanisms are in place, the accessibility of data, specifically under contingency plan execution, is subject to compromise.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) From Analyzer main Menu, go to 3;G. Record the SYSRES Volume serial number. From Administrator main Menu, go to 8;3. Enter PASSWORD in the Dsname Level field. Enter the SYSRES Volume serial number in the Volume serial field. <ENTER>.

b) If the message NO FILES MATCH DSN LVL is returned, there is NO FINDING.

c) If the PASSWORD dataset shows up on the report, this is a FINDING

Fix Text: System programmers will ensure that the old OS Password Protection is not used and any data protected by the old OS Password technology is removed and protection is replaced by the ACP.

Review the contents of the PASSWORD data set. Ensure that any protections it provides are provided by the ACP and delete the PASSWORD data set.

Access to data sets on z/OS systems can be protected using the OS password capability of MVS. This capability has been available in MVS for many years, and its use is commonly found in data centers. Since the advent of ACPs, the use of OS passwords for file protection has diminished, and is commonly considered archaic and of little use. The use of z/OS passwords is not supported by all the ACPs.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-34

Group Title: AAMV0450

Rule ID: SV-34r3_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0450](#)

Rule Title: System programs (e.g., exits, SVCs, etc.) must have approval of appropriate authority and/or documented correctly.

Vulnerability Discussion: Many vendor products and applications require or provide operating system exits, SVCs, I/O appendages, special PPT privileges, and APF authorization. Without proper review, approval and adequate documentation of these system programs, the integrity and availability of the operating system, ACP, and customer data are subject to compromise.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCPD-1

Check Content:

- a) From Analyzer main Menu, go to 4;B. Enter S next to APF tables. Enter YES next to AC(1) module list and NO to all other options in lower half of the screen. Submit the batch job. Refer to the report. Review any locally developed modules in the AC(1) list by APF authorized library per item (g) below.
- b) From Analyzer main Menu, go to 3;C. ENTER. Refer to online report. Ensure that any item with a YES under CMD, PGM or TSF is reviewed per item (g) below.
- c) From Analyzer main Menu, go to 4;E. Enter NO to all options on the screen. Submit the batch job. Refer to the report. If you see this in the report There are 0 User I/O Appendages defined for use. then no finding for I/O appendages. Otherwise, review the I/O appendages listed per item (g) below.
- d) From Analyzer main Menu, go to 4;J. Enter NO to all options on the screen. Submit the batch job. Refer to the report. Review all locally developed exits listed per item (g) below.
- e) From Analyzer main Menu, go to 4;A. Enter NO to all options on the screen. Submit the batch job. Refer to the report. Review all modules with SPEC KEY = YES, BYP PASS = YES or PROT KEY = 7 or less that was locally developed per item (g) below.
- f) From Analyzer main Menu, go to 4;D. Enter S next to all data sources. Enter NO to all options on the lower half of the screen. Submit the batch job. Refer to the report looking for any Locally Defined USER SVCs (Usually between 200 and 255) per item (g) below.
- g) Ensure the following items are in effect:
 - 1. The acquisition of any new IA and IA-enabled Commercial-Off-the-Shelf (COTS) products meets the applicable Common Criteria, NIAP, or FIPS evaluation and validation requirements specified in NSTISSP No. 11 and DODI 8500.2 or receives DAA approval.
 - 2. All locally developed extensions to the operating system environment (i.e., operating system exits, SVCs, I/O appendages, modules requiring special

PPT privileges and APF authorization) have been reviewed and approved by site DAA.

h) If both items in (g) are true for all system programs, there is NO FINDING.

i) If any item in (g) is untrue for a system program, this is a FINDING.

Fix Text: Ensure any new system software or major upgrade of software that performs any of the following actions:

- Runs authorized or with special privileges so it can use z/OS facilities restricted to authorized programs.
- Requires the use of a new Supervisor Call routine (SVC), Program Call routine (PC), installation exit routine, or I/O appendage routine.
- Modifies MVS in any way.
- Requires the use of the Authorized Program Facility (APF).
- Requires that the name of the program be placed in the MVS Program Properties Table (PPT).
- Runs in Supervisor State.
- Runs with a program status word (PSW) protection key between 0 through 7.
- Runs with a userid that has special security privileges within the ACP.

Has been approved by Common Criteria, NIAP, or FIPS evaluation and validation requirements specified in CNSSP No. 11 and DODD 8500.1 or receives DAA approval.

CCI: CCI-000271

CCI: CCI-000633

CCI: CCI-000634

CCI: CCI-001806

Group ID (Vulid): V-33795

Group Title: AAMV0500

Rule ID: SV-44220r3_rule

Severity: CAT II

Rule Version (STIG-ID): [AAMV0500](#)

Rule Title: Sensitive and critical system data sets exist on shared DASD.

Vulnerability Discussion: Any time a sensitive or critical system data set is allocated on a shared DASD device, it is critical to validate that it is properly protected on any additional systems that are sharing that device. Without proper review and adequate restrictions to access of these data sets on all systems sharing them, can lead to corruption, integrity and availability of the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-2, DCSL-1, ECAN-1, ECCD-1, ECCD-2

Check Content:

a) To get a list of all shared DASD:

- From Analyzer main menu, select option 4;O (DASD Analysis). This will generate a report of all DASD with a flag showing if it is shareable or not.
- On the VOLUME ANALYSIS menu that is presented, enter YES next to VTOC Analysis so that the list of datasets on each volume will be displayed.

b) Check the VTOC list of datasets for any critical or sensitive datasets (such as APF, LINKLIST, LPA, Catalog or Product-type Data sets).

c) The IAO and/or Systems programming personnel must confirm that there is a justification for having these data sets on shared DASD and that there is justification for the systems that have access to the shared DASD to access the critical/sensitive data sets that may be on them.

d) If (c) is true there is NO FINDING.

e) If (c) is not true there is a FINDING.

Fix Text: The System programming and system configuration personnel will review the list of shared DASD. Validate that identified volumes of shared DASD are still valid within the following.

HMC
VM
z/OS

If the shared volume(s) are valid and systems having access to these shared volume(s) are valid, map disk/VTOC list to obtain data sets on the shared volume(s). From this list obtain a list of sensitive and critical system data sets that are found on the shared volume(s). Ensure that the data sets are justified to be shared on the system and to reside on the shared volume(s).

The IAO will review all access requirements to validate that sensitive and critical system data sets are protected from unauthorized access across all systems that have access to the shared volume(s). Protecting the data set(s) whether the data set(s) are used or not used on the systems that have the shared volume(s) available to them.

CCI: CCI-000099

CCI: CCI-001090

CCI: CCI-001414

Group ID (Vulid): V-130

Group Title: ACF0250

Rule ID: SV-130r3_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0250](#)

Rule Title: The APPLDEF GSO record if used must have supporting documentation indicating the reason it was used.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

The IAO will ensure that certificate name filtering is not used unless the filtering rules have been documented to, and approved by, the IAM.

Currently the RACDCERT command does not support a generic userid value of ID(*) LISTMAP to list all the certificate name filters defined to RACF. However, the following commands can be issued to determine if certificate name filtering may be implemented.

- a) If certificate name filtering is in use, collect documentation describing each active filter rule and written approval from the ISSM to use the rule.
- b) Issue the SETROPTS LIST command. If the DIGTNMAP resource class is active, RACF is ready to process any certificate name filters with a Status of TRUST. The DIGTNMAP resource class should not be active unless certificate name filtering is desired.

If the DIGTNMAP resource class is not active, there is NO FINDING.

- c) Certificate name filters are stored as profiles in the DIGTNMAP resource class. The RLIST command is not intended for use with profiles in the DIGTNMAP resource class. However it can be used to determine if any profiles are defined. (NOTE: The information will not be displayed in a suitable format to easily interpret the filter.)

RLIST DIGTNMAP *

If there is nothing to list in the DIGTNMAP resource class, there is NO FINDING.

If profile information is displayed, one or more certificate name filters are defined to RACF. Under the NAME heading of each profile listing is the userid the filter is being mapped to. Issue the following command the list the certificate name filter associated with each userid:

Using Vanguard Administrators View Digital Mapping Filters option 18;2 with no masking review all Certificate name filters.

NOTE: Certificate name filters are only valid when their Status is TRUST. Therefore, you may ignore filters with the NOTRUST status.

- d) If the DIGTNMAP resource class is active and certificate name filters have a Status of TRUST, certificate name filtering is in use.
- e) If certificate name filtering is in use and filtering rules have been documented and approved by the ISSM, there is NO FINDING.
- f) If certificate name filtering is in use and filtering rules have not been documented and approved by the ISSM, this is a FINDING.

Fix Text: Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect APF Authorized Libraries.

Ensure that WRITE or greater access to libraries included in the system REXXLIB concatenation is limited to system programmers only.

Ensure READ access is allowed on to appropriate Started Tasks and Auditors.

Ensure UPDATE and/or ALTER access (i.e., successes and failures) is logged.

CCI: CCI-000366

CCI: CCI-000368

Group ID (Vulid): V-131

Group Title: ACF0260

Rule ID: SV-131r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0260](#)

Rule Title: The AUTHEXIT GSO record value is used to define an extended user authentication exit at TSO logon, for Operator Identification (OID) card usage. DISA requires the use of NCPASS on all of its domains.

Vulnerability Discussion: The AUTHEXIT GSO record value is used to define an extended user authentication exit at TSO logon, for Operator Identification (OID) card usage. DISA requires the use of NCPASS on all of its domains. DISA sites require the use of AUTHEXIT for other non DISA sites this value is optional.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
 2. Press ENTER
 3. Verify that If the GSO AUTHEXIT values conform to the following DISA requirements
LIDFIELD(AUTHSUP1) PROCPGM(AUTHXNCP) NOINFOSTG
- b) If the GSO APPLDEF record does not exist, there is NO FINDING.

c) If the GSO APPLDEF record does exist and no supporting documentation is available, this is a FINDING.

Fix Text:

The IAO will ensure that the AUTHEXIT GSO value is used to define an extended user authentication exit at TSO logon. For Operator Identification (OID) card usage. DISA requires the use of NCPASS on all of its domains. DISA sites require the use of AUTHEXIT for other non DISA sites this value is optional.

Ensure the GSO AUTHEXIT record values conform to the following DISA requirements.

GSO AUTHEXIT.001 record: LIDFIELD(AUTHSUP1) PROCPGM(AUTHXNCP) NOINFOSTG

Example:

```
SET C(GSO)
INSERT AUTHEXIT.001 NOINFOSTG LIDFIELD(AUTHSUP1) PROCPGM(AUTHXNCP)
```

```
F ACF2,REFRESH(AUTHEXIT)
```

CCI: CCI-000764

CCI: CCI-000765

Group ID (Vulid): V-132

Group Title: ACF0270

Rule ID: SV-132r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0270](#)

Rule Title: The AUTOERAS GSO record value must be set to indicate that ACF2 is controlling the automatic physical erasure of VSAM or non VSAM data sets.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. Verify that If the GSO AUTOERAS values conform to the following DISA requirements
All Systems: NON-VSAM VSAM VOLS(-)

b) If the GSO AUTOERAS record does not exist, there is NO FINDING.

c) If the GSO AUTOERAS record does exist and no supporting documentation is available, this is a FINDING.

Fix Text:

The IAO must ensure that the AUTOERASE GSO value indicates that ACF2 is controlling the automatic physical erasure of VSAM or non VSAM data sets.

Example:

```
SET C(GSO)
INSERT AUTOERAS NON-VSAM VSAM VOLS(-)
```

```
F ACF2,REFRESH(AUTOERAS)
```

CCI: CCI-001028

CCI: CCI-001090

Group ID (Vulid): V-133

Group Title: ACF0280

Rule ID: SV-133r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0280](#)

Rule Title: The BACKUP GSO record value specifies a time field and Time(00:00) is not specified unless the database is shared and backed up on another system.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

3. Verify that If the GSO AUTOERAS values conform to the following DISA requirements
CPUID() PRISPACE(5) SECSPACE(5) STRING(S ACFBKUP) TIME(00:01) WORKUNIT(VIO)

b) If the GSO AUTOERAS record does not exist, there is NO FINDING.

c) If the GSO AUTOERAS record does exist and no supporting documentation is available, this is a FINDING.

Fix Text:

The IAO will ensure that the BACKUP GSO value specifies a time field and Time(00:00) is not specified unless the database is shared and backed up on another system.

CPUID() PRISPACE(5) SECSPACE(5) STRING(S ACFBKUP) TIME(00:01) WORKUNIT(VIO)

Example:

SET C(GSO)

INSERT BACKUP CPUID() PRISPACE(5) SECSPACE(5) STRING(S ACFBKUP) TIME(00:01) WORKUNIT(VIO)

F ACF2,REFRESH(BACKUP)

CCI: CCI-000537

Group ID (Vulid): V-134

Group Title: ACF0290

Rule ID: SV-134r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0290](#)

Rule Title: The BLPPGM GSO record value indicates that ACF2 does not control the programs authorized to use tape bypass label processing (BLP).

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. Verify that If the GSO BLPPGM record is not defined, there is NO FINDING.
4. If the GSO BLPPGM record is defined, this is a FINDING.

Fix Text:

The IAO will ensure the BLPPGM GSO value indicates that ACF2 does not control the programs authorized to use tape bypass label processing (BLP).

NOTE: BLP enforcement will be done based on LID record settings.

Example:

SET C(GSO)
LIST BLPPGM
ACF0A005 RECORD(S) NOT FOUND

CCI: CCI-000382

CCI: CCI-001764

Group ID (Vulid): V-135

Group Title: ACF0300

Rule ID: SV-135r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0300](#)

Rule Title: The CLASMAP GSO record value translates an eight-character SAF resource class into a three character ACF2 resource type code to enable resource rules to be written to perform validation. Also it translates the resource type codes for ACF2 calls or calls made to ACF2 from CA's International Standard Security Facility (CAISSF). Vendor defaults as

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. If the GSO CLASMAP record values conform to the following requirements, there is NO FINDING.

Translates an eight-character SAF resource class into a three character ACF2 resource type code to enable resource rules to be written to perform validation. Also it translates the resource type codes for ACF2 calls or calls made to ACF2 from CA's International Standard Security Facility (CAISSF). Vendor defaults as

specified in the internal CLASMAP records unless as indicated otherwise below. The following resource class to resource type translations are the recommended standard: APPL maps to APL, CONSOLE maps to CON, FACILITY maps to FAC, OPERCMDS maps to OPR, and TSOAUTH maps to TSO

c) If there is any deviation from the above requirements in the GSO CLASMAP record values, this is a FINDING.

Fix Text:

The IAO will ensure the CLASMAP GSO value translates an eight-character SAF resource class into a three character ACF2 resource type code.

Translates an eight-character SAF resource class into a three character ACF2 resource type code to enable resource rules to be written to perform validation. Also it translates the resource type codes for ACF2 calls or calls made to ACF2 from CA's International Standard Security Facility (CAISSF).

Vendor defaults as specified in the internal CLASMAP records unless as indicated otherwise below.

The following resource class to resource type translations are the recommended standard:

APPL maps to APL
CONSOLE maps to CON
FACILITY maps to FAC
OPERCMDs maps to OPR
TSOAUTH maps to TSO

Example:

SHOW CLASMAP

CCI: CCI-000213

CCI: CCI-000366

Group ID (Vulid): V-136

Group Title: ACF0310

Rule ID: SV-136r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0310](#)

Rule Title: The EXITS GSO record value must specify the module names of site written ACF2 exit routines.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

If the GSO EXITS record values conform to the following requirements, there is NO FINDING.

Specifies the module names of site written ACF2 exit routines.

NOTE: The DSNPOST exit is optional and is not required to be specified in the GSO EXITS record. DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01)

NOTE: No other exits are authorized at this time.

NOTE: Local changes will be documented in writing with supporting documentation.

3. If there is any deviation from the above requirements in the GSO EXITS record values, this is a FINDING.

Fix Text:

The IAO will ensure the EXITS GSO value specifies the module names of site written ACF2 exit routines.

Specifies the module names of site written ACF2 exit routines.

NOTE: The DSNPOST exit is optional and is not required to be specified in the GSO EXITS record.

DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01)

Example:

SET C(GSO)
INSERT EXITS DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01)

F ACF2,REFRESH(EXITS)

NOTE: No other exits are authorized at this time.

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000021

CCI: CCI-000366

CCI: CCI-000368

CCI: CCI-000764

CCI: CCI-000765

CCI: CCI-001764

Group ID (Vulid): V-138

Group Title: ACF0330

Rule ID: SV-138r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0330](#)

Rule Title: The LINKLST GSO record value if specified only contains trusted system datasets.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the

security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO LINKLST record values conform to the following requirements, there is NO FINDING.

Specifies one or more partitioned data sets considered part of the system link (SYS1.LINKLIB) during data set access validation. Only trusted system data sets will be listed. Application libraries will never be included. Example: LIBRARY(SYS1.LINKLIB SYS2A.FDR.LOADLIB)

c) If there is any deviation from the above requirements in the GSO LINKLST record values, this is a FINDING.

Fix Text:

The IAO will ensure the LINKLIST GSO value if specified only contains trusted system datasets.

Specifies one or more partitioned data sets considered part of the system link (SYS1.LINKLIB) during data set access validation.

Only trusted system data sets will be listed. Application libraries will never be included.

Example:

```
SET C(GSO)
INSERT LINKLST LIBRARY(SYS1.LINKLIB SYS2A.FDR.LOADLIB)
```

```
F ACF2,REFRESH(LINKLST)
```

CCI: CCI-001762

CCI: CCI-001764

CCI: CCI-002342

Group ID (Vulid): V-140

Group Title: ACF0350

Rule ID: SV-140r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0350](#)

Rule Title: The MAINT GSO record value if specified will be restricted to production storage management user accounts and programs.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. If the GSO MAINT record values conform to the following requirements, there is NO FINDING.

Specifies the logonid, program, and library combinations used for system maintenance functions. NOTE: For logonids that match environments described in records, no SMF logging records will be created. NOTE: Entries will be restricted to production storage management user accounts and programs.

4. If there is any deviation from the above requirements in the GSO MAINT record values, this is a FINDING.

Fix Text:

The IAO will ensure the MAINT GSO value if specified will be restricted to production storage management user accounts and programs.

Specifies the logonid, program, and library combinations used for system maintenance functions.

NOTE: For logonids that match environments described in records, no SMF logging records will be created.

NOTE: Entries will be restricted to production storage management user accounts and programs.

CCI: CCI-001762

CCI: CCI-001764

CCI: CCI-002262

Group ID (Vulid): V-141

Group Title: ACF0360

Rule ID: SV-00000r0_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0360](#)

Rule Title: The NJE GSO record value must indicate validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is

found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration

2. Press ENTER

3. If the GSO NJE record values conform to the following requirement

SSpecifies ACF2 validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).

Example: DFTLID() INHERIT NODEMASK(-) ENCRYPT VALIN(YES) NOVALOUT

NOTE: For NJE nodes that are incompatible with the XDES algorithm, discrete NJE records will be created with NOENCRYPT.

NOTE: Local changes will be documented in writing with supporting documentation.

b) If the GSO NJE record values conform to the following requirements, there is NO FINDING.

c) If there is any deviation from the above requirements in the GSO NJE record values, this is a FINDING.

Fix Text:

The IAO will ensure that the NJE GSO value indicates validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).

Specifies ACF2 validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).

Example:

DFTLID()
INHERIT
NODEMASK(-)
ENCRYPT
VALIN(YES)
NOVALOUT

NOTE: For NJE nodes that are incompatible with the XDES algorithm, discrete NJE records will be created with NOENCRYPT.

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000213

CCI: CCI-001414

CCI: CCI-001762

CCI: CCI-001764

CCI: CCI-002314

Group ID (Vulid): V-142

Group Title: ACF0370

Rule ID: SV-00000r0_rule

Severity: CAT I

Rule Version (STIG-ID): [ACF0370](#)

Rule Title: The OPTS GSO record value must be set to the values specified.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. If the GSO OPTS record value conforms to the following requirement, this is not a finding.

MODE(ABORT)

4.

Examples of a Category I FINDING where no further analysis is required:

MODE(WARN)

MODE(LOG)

MODE(QUIET)

Example of a possible Category I FINDING requiring additional analysis:

MODE(RULE,norule,no\$mode)

norule specifies the action (i.e., QUIET, LOG, WARN, and ABORT) for a data set access request if no rule set is found.

no\$mode specifies the action (i.e., QUIET, LOG, WARN, and ABORT) for a data set access request if no \$MODE control statement is found in a rule set.

Possible scenarios justifying a downgrade to a Category II:

If some sensitive data sets are not protected by rules sets and norule is set to QUIET, LOG, or WARN, unauthorized access may result for these unprotected data sets.

If rule sets for some sensitive data sets have \$MODE set to QUIET, LOG, or WARN, unauthorized access may result for the data sets protected by these rule sets.

If rule sets for some sensitive data sets have \$MODE missing and no\$mode is QUIET, LOG, or WARN, unauthorized access may result for the data sets protected by these rule sets.

Fix Text:

The IAO will ensure that the OPTS GSO value is set to valid options.

Define the global options available to the system.

MODE(ABORT)

Example:

```
SET C(GSO)
INSERT OPTS BLPLOG NOCACHE NOCMDREC CONSOLE(NOROLL) CPUTIME(LOCAL) DATE(MDY) NODDB DFTLID() DFTSTC()
INFOLIST(SEcurity, AUDIT) JOBCHK MAXVIO(10)
MODE(ABORT) NOTIFY RPTSCOPE SHRDASD STAMPSMF STC TAPEDSN TEMPDSN NOUADS NOVTAMOPEN

F ACF2,REFRESH(OPTS)
```

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-36899

Group Title: ACF0375

Rule ID: SV-48660r5_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0375](#)

Rule Title: The OPTS GSO record value must be set to the values specified.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

3. If the GSO OPTS record values conform to the following requirements, this is not a finding.

BLPLOG
NOCMDREC
CONSOLE(NOROLL)
CPUTIME(LOCAL)
DATE(MDY)
NODDB
DFTLID()
DFTSTC()
INFOLIST(none | AUDIT | SECURITY | SECURITY, AUDIT)
JOBCHK
MAXVIO(10)
NOTIFY
RPTSCOPE
SHRDASD
STAMPSMF
STC
TAPEDSN
TEMPDSN
NOUADS
NOVTAMOPEN

c) If the GSO OPTS record values DO NOT conform to the following requirements, this is a FINDING.

Fix Text:

Ensure that the GSO OPTS value is set to valid options. This will also include the GSO OPTS MODE setting from ACF0370.

Define the global options available to the system.

BLPLOG
NOCMDREC
CONSOLE(NOROLL)
CPUTIME(LOCAL)
DATE(MDY)
NODDB
DFTLID()
DFTSTC()
INFOLIST(none | AUDIT | SECURITY | SECURITY, AUDIT)
JOBCHK

MAXVIO(10)
NOTIFY
RPTSCOPE
SHRDASD
STAMPSMF
STC
TAPEDSN
TEMPDSN
NOUADS
NOVTAMOPEN

Example:

SET C(GSO)
INSERT OPTS BLPLOG NOCMDREC CONSOLE(NOROLL) CPUTIME(LOCAL) DATE(MDY) NODDB DFTLID() DFTSTC() INFOLIST(SEcurity,
AUDIT) JOBCHK MAXVIO(10)
MODE(ABORT) NOTIFY RPTSCOPE SHRDASD STAMPSMF STC TAPEDSN TEMPDSN NOUADS NOVTAMOPEN

F ACF2,REFRESH(OPTS)

CCI: CCI-000366

CCI: CCI-001762

CCI: CCI-001764

Group ID (Vulid): V-143

Group Title: ACF0380

Rule ID: SV-143r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0380](#)

Rule Title: The PPGM GSO record value must indicate protected programs that are only executed by privileged users.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. Compare the GSO PPGM record values with the programs:

Check the SENSITIVE UTILITY CONTROLS Table is located in the Z/OS Addendum.

b) If all applicable programs or their generic equivalent referenced in (b) above are represented by GSO PPGM record values, there is NO FINDING.

c) If any applicable program referenced in (b) above is not represented by a GSO PPGM record value, this is a FINDING.

Fix Text:

The IAO will ensure that the PPGM GSO value indicates protected programs that are only executed by privileged users.

Check the SENSITIVE UTILITY CONTROLS Table in the zOS STIG Addendum.

Define protected programs that can only be executed by privileged users.

PGM MASK(pgm mask1, ...,pgm-mask255)

Example:

SET C(GSO)

INSERT PPGM PGM-MASK(<program name or generic equivalent>)

F ACF2,REFRESH(PPGM)

CCI: CCI-002235

Group ID (Vulid): V-144

Group Title: ACF0390

Rule ID: SV-144r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0390](#)

Rule Title: The PSWD GSO record values must be set to the values specified in the checks portion below.

Vulnerability Discussion: Password complexity, or strength, is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that need to be tested before the password is compromised. Use of a complex password helps to increase the time and resources required to compromise the password.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
3. The GSO PSWD record will conform to the following requirements.

MAXTRY(3)

MINPSWD(8)

PASSLMT(3)

PSWDALPH

PSWDALT

PSWDFRC

PSWDHST

PSWDJES

PSWDLCL
PSWDLID
PSWDMAX(1-60)
PSWDMIN(1)
PSWDMIXD
PSWDNAME(4)
PSWDNCH
PSWDNMIC
PSWDNUM
PSWDPAIR(0)
PSWDPLID
PSWDPLST(Special character list as defined in CA ACF2 for z/OS Administration Guide)
PSWDREQ
PSWDRSV (Reserve list is located in the addendum Section 5.1.3)
PSWDSIM(3)
PSWDSPLT
PSWDUC
PSWDVOWL
NOPSWDXTR
PSWXHIST
PSWXHST#(10-64)
WRNDAYS (10)

b) If the GSO PSWD record will conform to the following requirements This is a NO FINDING

c) If the GSO PSWD record do not conform to the following requirements This is a FINDING

Fix Text:

Ensure that the PSWD GSO values are set to the values specified.

Note: Current DoD policy has changed requiring that the password change interval be at the most 60 days.

Ensure the GSO PSWD record values conform to the following requirements.

MAXTRY(3)
MINPSWD(8)
PASSLMT(3)
PSWDALPH
PSWDALT

PSWDFRC
PSWDHST
PSWDJES
PSWDLCL
PSWDLID
PSWDMAX(1-60)
PSWDMIN(1)
PSWDMIXD
PSWDNAME(4)
PSWDNCH
PSWDNMIC
PSWDNUM
PSWDPAIR(0)
PSWDPLID
PSWDPLST(special character list as defined in CA ACF2 for z/OS Administration Guide)
PSWDREQ
PSWDRSV (Reserve list is located in the addendum Section 5.1.3)
PSWDSIM(3)
PSWDSPLT
PSWDUC
PSWDVOWL
NOPSWDXTR
PSWXHIST
PSWXHST#(10-64)
WRNDAYS(10)
Example:

SET C(GSO)
INSERT PSWD MAXTRY(3) MINPSWD(8) PASSLMT(3) PSWDALPH PSWDALT PSWDFRC PSWDHST PSWDJES PSWDLCL PSWDLID
PSWDMAX(60) PSWDMIN(1) PSWDMIXD PSWDNAME(4) PSWDNCH PSWDNMIC PSWDNUM PSWDPAIR(0) PSWDPLID PSWDPLST() PSWDREQ
PSWDRSV PSWDSIM(3) PSWDSPLT PSWDUC NOPSWDVFY PSWDVOWL NOPSWDXTR NOPSWNAGE PSWXHIST PSWXHST#(10)
WRNDAYS(10)

F ACF2,REFRESH(PSWD)

CCI: CCI-000044

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000198

CCI: CCI-000199

CCI: CCI-000200

CCI: CCI-000205

CCI: CCI-001619

CCI: CCI-002238

Group ID (Vulid): V-145

Group Title: ACF0400

Rule ID: SV-48576r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0400](#)

Rule Title: The PWPHRASE GSO record must be properly defined.

Vulnerability Discussion: Sites may opt to use passphrases in lieu of passwords for authentication. A passphrase must nevertheless be constrained by certain complexity parameters to assure appropriate strength. The GSO PWPHRASE record specifies the rules that ACF2 will apply when a user selects a new password

phrase.

The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration

2. Press ENTER

Note: Current DoD policy has changed requiring that the password change interval be at the most 60 days. Ensure that this is in effect.

3. The GSO PWPHRASE record will conform to the following requirements.

ALPHA(1 or greater)

HISTORY(10-32)

MAXDAYS(1-60)

MINDAYS(1)

MINLEN(15-100)

NUMERIC(1 or greater)

SPECIAL(1 or greater)

SPECLIST() or SPECLIST(character list)

WARNDAYS(1-10)

Note: The SPECLIST special characters will be specified at a minimum. Characters will conform to the allowable list defined in CA ACF2 for z/OS Administration Guide.

b) If the GSO PWPHRASE record conforms, there is NO FINDING.

c) If the GSO PWPHRASE record does not conform this is a FINDING.

Fix Text:

The IAO will ensure that the PWPHRASE GSO values are set to the values specified.

Note: Current DoD policy has changed requiring that the password change interval be at the most 60 days.

Ensure the GSO PWPHRASE record values conform to the following requirements.

ALPHA(1 or greater)
HISTORY(10-32)
MAXDAYS(1-60)
MINDAYS(1)
MINLEN(15-100)
NUMERIC(1 or greater)
SPECIAL(1 or greater)
SPECLIST() or SPECLIST(character list)
WARNDAYS(1-10)

Note: The SPECLIST special characters will be specified at a minimum. Characters will conform to the allowable list defined in CA ACF2 for z/OS Administration Guide.

Example:

SET C(GSO)
INSERT PWPHRASE NOALLOW ALPHA(1) HISTORY(10) MAXDAYS(60) MINDAYS(1) MINLEN(15) NUMERIC(1) SPECIAL(1) SPECLIST(& * =)
WARNDAYS(10)

F ACF2,REFRESH(PWPHRASE)

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000198

CCI: CCI-000199

CCI: CCI-000200

CCI: CCI-000205

CCI: CCI-001395

CCI: CCI-001619

Group ID (Vulid): V-146

Group Title: ACF0410

Rule ID: SV-146r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0410](#)

Rule Title: The RESRULE GSO record value is set to NONE any other setting requires documentation justifying the change.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO RESRULE record values conform to the following requirements, there is NO FINDING.

None.

NOTE: Local changes will be documented in writing with supporting documentation.

c) If there is any deviation from the above requirements in the GSO RESRULE record values, this is a FINDING.

Fix Text:

The IAO will ensure that the RESRULE GSO value is set to NONE any other setting requires documentation justifying the change.

Ensure the GSO RESRULE record values conform to the following requirements.

None.

Example:

```
SET C(GSO)
INSERT RESRULE INDEX()

F ACF2,REFRESH(RESRULE)
```

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000366

CCI: CCI-000368

CCI: CCI-000369

Group ID (Vulid): V-147
Group Title: ACF0420
Rule ID: SV-147r2_rule
Severity: CAT II
Rule Version (STIG-ID): [ACF0420](#)

Rule Title: The RESVOLS GSO record value is set to Volmask(-). Any other setting requires documentation justifying the change.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO RESVOLS record values conform to the following requirements, there is NO FINDING.

VOLMASK(-)

NOTE: Local changes will be documented in writing with supporting documentation.

c) If there is any deviation from the above requirements in the GSO RESVOLS record values, this is a FINDING.

Fix Text:

The IAO will ensure that the RESVOL GSO value is set to Volmask(-). Any other setting requires documentation justifying the change.

Ensure the GSO RESVOLS record values conform to the following requirements.

VOLMASK(-)

Example:

SET C(GSO)

INSERT RESVOLS VOLMASK(-)

F ACF2,REFRESH(RESVOLS)

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000368

CCI: CCI-000369

CCI: CCI-001199

CCI: CCI-001399

Group ID (Vulid): V-148

Group Title: ACF0430

Rule ID: SV-148r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0430](#)

Rule Title: The RULEOPTS GSO record values are set to the values specified.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration

2. Press ENTER

B. VVerify that the GSO RULEOPTS record have the following options. If the following options are defined, this is not a finding.

NO\$NOSORT

CENTRAL

CHANGE

NOCOMPDYN

DECOMP(AUDIT SECURITY) | DECOMP(AUDIT) | DECOMP(SEcurity)

NORULELONG

c) Verify that the GSO RULEOPTS record have the following options. If the following options are not defined, this is a FINDING

Fix Text:

The IAO will ensure that the RULEOPTS GSO values are have the proper options specified.

Ensure the GSO RULEOPTS record values conform to the following requirements.

NO\$NOSORT

CENTRAL

CHANGE

NOCOMPDYN

DECOMP(AUDIT SECURITY) | DECOMP(AUDIT) | DECOMP(SEcurity)

NORULELONG

Example:

SET C(GSO)

INSERT RULEOPTS NO\$NOSORT CENTRAL CHANGE NOCOMPDYN DECOMP(AUDIT SECURITY) NORULELONG

F ACF2,REFRESH(RULEOPTS)

CCI: CCI-000366

CCI: CCI-000368

CCI: CCI-000369

Group ID (Vulid): V-149

Group Title: ACF0440

Rule ID: SV-149r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0440](#)

Rule Title: The SAFDEF GSO record baseline values are not are set to the values previously documented.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO SAFDEF record values conform to the following requirements, there is NO FINDING.

Vendor defaults as specified in the internal SAFDEF records.

NOTE: All vendor-modified and site-defined SAFDEF records will be documented in writing with supporting documentation.

c) If there is any deviation from the above requirements in the GSO SAFDEF record values, this is a FINDING.

Fix Text:

The IAO will ensure that the SAFDEF GSO values are set to the values specified.

Defines System Authorization Facility (SAF) calls that each site may want to process differently than the default ACF2 process.

Vendor defaults as specified in the internal SAFDEF records.

NOTE: All vendor-modified and site-defined SAFDEF records will be justified in writing with supporting documentation.

CCI: CCI-000213

CCI: CCI-000368

CCI: CCI-000369

Group ID (Vulid): V-00000

Group Title: ACF0480

Rule ID: SV-150r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0480](#)

Rule Title: The SECVOLS GSO record value is set to VOLMASK(). Any local changes are justified and documented with the IAO.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
- b) If the GSO SECVOLS record values conform to the following requirements, there is NO FINDING.

VOLMASK()

NOTE: Local changes will be documented in writing with supporting documentation.

- c) If there is any deviation from the above requirements in the GSO SECVOLS record values, this is a FINDING.

Fix Text:

The IAO will ensure that the SECVOLS GSO value is set to VOLMASK(). Any local changes are justified and documented with the IAO.

Defines those DASD, mass storage, and tape volumes for which ACF2 is to provide volume level protection.

Ensure the GSO SECVOLS record values conform to the following requirements.

VOLMASK()

Example:

SET C(GSO)
INSERT SECVOLS VOLMASK()

F ACF2,REFRESH(SECVOLS)

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000368

CCI: CCI-000369

CCI: CCI-001199

CCI: CCI-001399

Group ID (Vulid): V-151

Group Title: ACF0490

Rule ID: SV-151r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0490](#)

Rule Title: The SYNCOPTS GSO record values are set to the values specified.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO SYNCOPTS record values conform to the following requirements, there is NO FINDING.

FILENAME(ACF2.SYNCFIL) POLLINTV(10) USECOUNT(10) NOACTIVATE

c) If there is any deviation from the above requirements in the GSO SYNCOPTS record values, this is a FINDING.

Fix Text:

The IAO will ensure that the SYNCOPTS GSO values are set to the values specified.

Defines the cache synchronization processing for a CPU running in a shared ACF2 database environment.

Ensure the GSO SYNCOPTS record values conform to the following requirements.

FILENAME(ACF2.SYNCFILE) POLLINTV(10) USECOUNT(10) NOACTIVATE

Example:

```
SET C(GSO)
INSERT SYNOPTS NOACTIVATE FILENAME(ACF2.SYNCFILE) POLLINTV(10) USECOUNT(10)

F ACF2,REFRESH(SYNOPTS)
```

CCI: CCI-000366

CCI: CCI-002357

Group ID (Vulid): V-152

Group Title: ACF0500

Rule ID: SV-152r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0500](#)

Rule Title: The TSO GSO record values must be set to the values specified.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

ACCOUNT(1)

BYPASS(#)
CHAR(BS)
CMDLIST()
NOIKJEFLD1
LINE(ATTN)
LOGONCK
PERFORM(0)
PROC(site defined)
NOQLOGON
REGION(site defined)
SUBCLSS()
SUBHOLD()
SUBMSG()
TIME(0)
TSOSOUT(A)
UNIT(SYSDA)
WAITIME(60) or less

Fix Text:

The IAO will ensure that the TSO GSO values are set to the values specified.

Ensure the GSO TSO record values conform to the following requirements.

ACCOUNT(1)
BYPASS(#)
CHAR(BS)
CMDLIST()
NOIKJEFLD1
LINE(ATTN)
LOGONCK
PERFORM(0)
PROC(site defined)
NOQLOGON
REGION(site defined)
SUBCLSS()
SUBHOLD()
SUBMSGC()
TIME(0)

TSOSOUT(A)
UNIT(SYSDA)
WAITIME(60) or less

Example:

SET C(GSO)
INSERT TSO ACCOUNT(1) BYPASS(#) CHAR(BS) CMDLIST() NOIKJEFLD1 LINE(ATTN) LOGONCK PERFORM(0) PROC(IKJACCNT)
NOQLOGON REGION(4,096) SUBCLSS() SUBHOLD() SUBMSGC() TIME(0) TSOGNAME() TSOSOUT(A) UNIT(SYSDA) WAITIME(60)

F ACF2,REFRESH(TSO)

CCI: CCI-000366

CCI: CCI-001133

Group ID (Vulid): V-153

Group Title: ACF0510

Rule ID: SV-153r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0510](#)

Rule Title: The TSOCRT GSO record values are set to the appropriate values.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER
- PDI(ACF0510)

b) If the GSO TSOCRT record values conform to the following requirements, there is NO FINDING.

STRING(A12FA11C1A270C0D)

c) If there is any deviation from the above requirements in the GSO TSOCRT record values, this is a FINDING.

Fix Text:

The IAO will ensure that the TSOCRT GSO values are set to the values specified.

Defines a clear string used to obliterate the logon to ASCII CRT devices.

STRING(A12FA11C1A270C0D)

Example:

```
SET C(GSO)
INSERT TSOCRT STRING(A12FA11C1A270C0D)
```

```
F ACF2,REFRESH(TSOCRT)
```

CCI: CCI-000206

Group ID (Vulid): V-154

Group Title: ACF0520

Rule ID: SV-154r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0520](#)

Rule Title: The TSOKEYS GSO record values specified are not in accordance with security requirements.

Vulnerability Discussion: (ACF0520: CAT II) The IAO will ensure that the TSOKEYS GSO value is set to KEYWORDS()....

The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system

environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO TSOKEYS record values conform to the following requirements, there is NO FINDING.

KEYWORDS()

c) If there is any deviation from the above requirements in the GSO TSOKEYS record values, this is a FINDING.

Fix Text:

The IAO will ensure that the TSOKEYS GSO value is set to KEYWORDS().

Defines site supplied keywords permitted by ACF2 at TSO logon time.

Ensure the GSO TSOKEYS record values conform to the following requirements.

KEYWORDS()

Example:

SET C(GSO)

INSERT TSOKEYS KEYWORDS()

F ACF2,REFRESH(TSOKEYS)

CCI: CCI-000366

Group ID (Vulid): V-155

Group Title: ACF0530

Rule ID: SV-155r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0530](#)

Rule Title: The TSOTWX GSO record values are set to the values specified.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) If the GSO TSOTWX record values conform to the following requirements, there is NO FINDING.

CR(15)
IDLE(17)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

c) If there is any deviation from the above requirements in the GSO TSOTWX record values, this is a FINDING.

Fix Text:

The IAO will ensure that the TSOTWX GSO values are set to the values specified.

Defines a cross out mask to obliterate the logon password on TWX devices.

CR(15)
IDLE(17)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

Example:

SET C(GSO)
INSERT TSOTWX CR(15) IDLE(17) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()

F ACF2,REFRESH(TSOTWX)

CCI: CCI-000206

Group ID (Vulid): V-156

Group Title: ACF0540

Rule ID: SV-156r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0540](#)

Rule Title: The TSO2741 GSO record values specified are not in accordance with the proper security requirements.

Vulnerability Discussion: The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration

2. Press ENTER

b) If the GSO TSO2741 record values conform to the following requirements, there is NO FINDING.

BS(16)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

c) If there is any deviation from the above requirements in the GSO TSO2741 record values, this is a FINDING.

Fix Text:

The IAO will ensure that the TSO2741 GSO values are set to the values specified.

Defines a cross out string used to obliterate the logon password on 2741 devices.

Ensure the GSO TSO2741 record values conform to the following requirements.

BS(16)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

Example:

SET C(GSO)
INSERT TSO2741 BS(16) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()

F ACF2,REFRESH(TSO2741)

CCI: CCI-000206

Group ID (Vulid): V-158

Group Title: ACF0560

Rule ID: SV-158r3_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0560](#)

Rule Title: There are LOGONIDs defined to ACF2 that do not have the required fields completed.

Vulnerability Discussion: Within the LOGONID record, the users name and UID-string fields must be completed to ensure individual user accountability.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

b) Verify that the below listed fields are complete for all logonids. If the following guidance is true, this is not a finding.

NAME User's name

UID-String All fields defined in the ACFFDR @UID macro

NOTE: A completed NAME field that can either be traced back to a current DD2875 or a Vendor Requirement (example: A Started Task).

NOTE: A user may be required to have more than one logonid but users must not share userids.

Fix Text:

The IAO will ensure that all LOGONID records have the required attributes.

Review all LOGONID definitions to ensure required information is provided.

Every user will be identified to ACF2 via a unique userid. (ACF2 calls this a logonid.) To ACF2, a user is an individual, a started task, or a batch job.

Every user will be fully identified within ACF2. Complete the following fields for every logonid:

NAME - User's name
UID-String - All fields defined in the ACFFDR @UID macro

All fields that comprise the standard UID string will be filled out for each user as a logonid is added.

Example:

SET LID
INSERT logonid UID(uid string) NAME(user name)

CCI: CCI-000764

CCI: CCI-000804

Group ID (Vulid): V-159
Group Title: ACF0570
Rule ID: SV-159r5_rule
Severity: CAT II
Rule Version (STIG-ID): [ACF0570](#)
Rule Title: Interactive LOGONIDs defined to ACF2 must have the required fields completed.

Vulnerability Discussion: Improper assignments of attributes in the LOGONID record may allow users excessive privileges resulting in unauthorized access.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:
Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(TSOUSERS)
- ACF2CMDS.RPT(MAXDAYS0)

- ACF2CMDS.RPT(MAXDAYS)
- ACF2CMDS.RPT(MINDAYS)

1. From Administrator main menu, select 4 GSO Administration
2. Press ENTER

Verify that the interactive userids are properly defined. If the following guidance is true, this is not a finding.

___ Ensure that all logonid record fields for interactive users are specified as in the table entitled INTERACTIVE USERS - ACF2, in the z/OS STIG Addendum.

___ Ensure that MAXDAYS is a value of 1 to 60 days.

Note: Current DoD policy has changed requiring that the password change interval is set to a value of 1 to 60. Ensure that this is in effect.

Note: FTP only process and server to server userids may have MAXDAYS(0) and LIDZMAX specified. These users must be identified in the FTPUSERS group in the Dialog Process or FTP in the name field. Additionally, these users must change their passwords on an annual basis.

Fix Text:

The IAO will review all interactive LOGONID records to ensure required information is provided. Evaluate the impact of correcting any deficiencies. Develop a plan of action and implement the required changes.

Review all LOGONID definitions to ensure required information is provided as in the table entitled INTERACTIVE USERS - ACF2, in the zOS STIG Addendum.

Note: Current DoD policy has changed requiring that the password change interval is set to a value of 1 to 60. Ensure that this is in effect.

Note: FTP only process and server to server userids may have MAXDAYS(0) and LIDZMAX specified. These users must be identified in the FTPUSERS group in the Dialog Process or FTP in the name field. Additionally, these users must change their passwords on an annual basis.

Example:

```
SET LID
INSERT logonid UID(uid string) NAME(user name) AUTHSUP1 MAXDAYS(60) MINDAYS(1)
```

CCI: CCI-000199

CCI: CCI-000764

Group ID (Vulid): V-160

Group Title: ACF0580

Rule ID: SV-160r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0580](#)

Rule Title: There are batch jobs with restricted LOGONIDs that do not have the PGM(xxxxxxx) and SUBAUTH attributes or the SOURCE(xxxxxxx) attribute assigned to the corresponding LOGONIDs.

Vulnerability Discussion: Unauthorized jobs may be introduced into the system. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, 1 User Administration
- 1 User Summary by Privilege
2. Press ENTER

b) If the logonids that are associated with batch jobs have the RESTRICT attribute, then the logonids must also have the PGM(xxxxxxx) and SUBAUTH attributes, or the SOURCE(xxxxxxx) attribute specified.

c) If all restricted logonids have the PGM(xxxxxxx) and SUBAUTH attributes, and/or the SOURCE(xxxxxxx) attribute, there is NO FINDING.

d) If the PGM(xxxxxxx) and SUBAUTH attributes or the SOURCE(xxxxxxx) attribute is not specified for any restricted logonids, this is a FINDING.

Fix Text:

Ensure associated LOGONIDs exist for all batch jobs and restrict access to required resources only.

All batch jobs scheduled via an automation process will use the //*LOGONID xxxxxxxx card in the JCL stream to identify the userid. Use restricted logonids with the following parameter coded:

RESTRICT

One or both of the following will also be specified:

PGM(xxxxxxxx) and SUBAUTH
SOURCE(xxxxxxxx)

The use of default IDs prevents the identification of tasks with individual users as mandated by policy, and prevents adequate accountability. Default IDs for batch processing will not be used.

The use of USER= can also be used in the jobcard to identify the userid to be used for a job's processing.

CCI: CCI-002145

Group ID (Vulid): V-161

Group Title: ACF0600

Rule ID: SV-161r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0600](#)

Rule Title: There are LOGONIDs assigned for started tasks that do not have the STC attribute specified in the associated LOGONID record.

Vulnerability Discussion: If a LOGONID for a started task does not have the STC attribute specified, this could result in system or application unavailability.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 1 User Summary by Privilege
2. Press ENTER
3. Select STC

b) Identify all logonids assigned to started tasks.

c) Review every logonid record assigned to started tasks to ensure each one has the STC attribute specified.

d) If all logonids identified as started tasks have the STC attribute specified, there is NO FINDING.

e) If any logonid identified as a started task does not have the STC attribute specified, this is a FINDING.

Fix Text:

The IAO will ensure that all logonid records assigned to started tasks have the STC attribute specified.

All started tasks will be assigned an individual logonid. The logonid for a Started Task Control (STC) will be granted the minimum privileges necessary for the STC to function. In addition to the default LID field settings, all STC logonids will have the following field setting:

STC

Example:

SET LID
INSERT logonid STC

CCI: CCI-002145

Group ID (Vulid): V-162

Group Title: ACF0610

Rule ID: SV-162r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0610](#)

Rule Title: There are LOGONIDs associated with started tasks that have the MUSASS requirement but do not have both the MUSASS and NO-SMC specified in corresponding LOGONID records.

Vulnerability Discussion: If the LOGONID does not have the MUSASS attribute specified, there is no individual accountability within the associated address space.

If NO-SMC is not specified the potential for VSAM data set corruption exists.

Responsibility: Information Assurance Officer

IAControls: F-27334r1_fix

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)
- ACF2CMDS.RPT(ATTMUASS)

1. Logon to ACF2 and issue the following command:

LIST IF(MUSASS)

2. Press ENTER

b) Identify the started tasks that have a Multi-User Single Address Space System (MUSASS) requirement.

c) If every logonid associated with a started task that has the MUSASS requirement has the MUSASS and NO-SMC attributes, there is NO FINDING.

d) If any logonid associated with a started task that has the MUSASS requirement does not have the MUSASS and NO-SMC attributes, this is a FINDING.

Fix Text:

The IAO will ensure that if the STC is a Multi User Single Address Space System (MUSASS), the STC logonid has the MUSASS and NO-SMC attributes.

If the started task (STC) is a Multi User Single Address Space System (MUSASS), the STC logonid will also have the following attributes:

MUSASS

NO-SMC

Example:

SET LID

INSERT logonid STC MUSASS NO-SMC

CCI: CCI-002145

Group ID (Vulid): V-163

Group Title: ACF0620

Rule ID: SV-163r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0620](#)

Rule Title: There are LOGONIDs associated with started tasks that have the MUSASS attribute and the requirement to submit jobs on behalf of its users but do

not have the JOBFROM attribute as required.

Vulnerability Discussion: Individual accountability will be lost when submitting a job.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTNOCNL)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0640)

1. Logon to Administrator :

1 User Administration

1 User Summary by Privilege

2. Press ENTER

b) Ensure that only logonids associated with trusted STCs have the NON-CNCL attribute specified.

TRUSTED STCs:

Certain started tasks perform critical operating system-related functions. The site can secure these started tasks in one of two ways:

1) By analyzing an STC's access requirements and granting the requisite accesses.

2) By considering these started tasks as trusted for the purpose of data set and resource access requests.

The list of approved trusted started tasks is found in the TRUSTED STARTED TASKS Table in the zOS STIG Addendum.

c) If (b) above is true, there is NO FINDING.

d) If (b) above is untrue, there is a FINDING.

Fix Text:

The IAO will ensure that if the Multi User Single Address Space System (MUSASS) has the requirement to submit jobs on behalf of its users, the STC logonid has the JOBFROM attribute specified.

If the Multi User Single Address Space System (MUSASS) has the requirement to submit jobs on behalf of its users, the STC logonid will also have the following attribute:

JOBFROM

Example:

SET LID
CHANGE logonid STC JOBFROM

CCI: CCI-002145

Group ID (Vulid): V-1

Group Title: ACF0640

Rule ID: SV-1r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0640](#)

Rule Title: There are started task LOGONIDs with the NON-CNCL attribute specified In the associated LOGONID record that are not listed as trusted and have not been specifically approved.

Vulnerability Discussion: The NON-CNCL privilege exempts the started tasks from security checking. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, and customer data

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTNOCNL)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0640)

a) Display display LOGONIDs with the NON-CNCL Information as follows:

1. Logon to ACF2 and issue the following command:

LIST IF(NON-CNCL)

2. Press ENTER

2) By analyzing an STC's access requirements and granting the requisite accesses.

3) By considering these started tasks as trusted for the purpose of data set and resource access requests.

The list of approved trusted started tasks is found in the TRUSTED STARTED TASKS Table in the zOS STIG Addendum.

c) If (b) above is true, there is NO FINDING.

d) If (b) above is untrue, there is a FINDING.

Fix Text:

Review all LOGONIDs with the NON-CNCL attribute. The IAO will ensure that only STCs in the trusted STC list can have the NON-CNCL attribute. The list of approved trusted STCs is found in the TRUSTED STARTED TASKS Table in the zOS STIG Addendum.

The use of default IDs prevents the identification of tasks with individual users as mandated by policy, and prevents adequate accountability. Default IDs for STCs will not be used.

Certain started tasks performing critical operating system related functions may be considered trusted for the purposes of data set and resource access requests. For these STCs all access requests will be honored. These STCs will be given the following attribute to facilitate access while logging any accesses they would not ordinarily be granted by the access rule sets:

NON-CNCL

Example:

SET LID

CHANGE logonid STC NON-CNCL

CCI: CCI-002145

Group ID (Vulid): V-166

Group Title: ACF0660

Rule ID: SV-166r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0660](#)

Rule Title: There are maintenance LOGONIDs that do not have corresponding GSO MAINT records.

Vulnerability Discussion: Users may execute programs without ACP security checking or auditing. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. Logon to ACF2 and issue the following command:
LIST IF(MAINT)
2. Press ENTER

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0670)
- b) If every GSO MAINT record has a corresponding maintenance logonid, there is NO FINDING.
- c) If any GSO MAINT record does not have a corresponding maintenance logonid, this is a FINDING.

Fix Text:

The IAO will ensure that an associated GSO maintenance record exists for each special user logonid identifying the program(s) that it is permitted to access and the library where the program(s) resides.

An associated GSO MAINT record will exist for each special user logonid, identifying the program(s) that it is permitted to access and the library where the program(s) resides.

Every maintenance logonid has a corresponding GSO MAINT record.

Example:

SET C(GSO)

INSERT MAINT.DFSMSHSM LIBRARY(SYS1.LINKLIB) LID(HSMDFDSS) PGM(ADRDSSU)

F ACF2,REFRESH(MAINT)

CCI: CCI-002145

CCI: CCI-002883

Group ID (Vulid): V-167

Group Title: ACF0670

Rule ID: SV-167r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0670](#)

Rule Title: There are GSO MAINT records that do not have corresponding maintenance LOGONIDs.

Vulnerability Discussion: LOGONIDs could be intentionally created that correspond to the GSO MAINT records. Then the maintenance programs could be used to gain unauthorized access to the system. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display Resource Class Information as follows:

1. From Administrator main menu, select 4 GSO Administration

2. Press ENTER

3. b) If every GSO MAINT record has a corresponding maintenance logonid, there is NO FINDING.

c) If any GSO MAINT record does not have a corresponding maintenance logonid, this is a FINDING.

Fix Text:

The IAO will ensure that an associated user logonid exists for each special GSO maintenance record identifying the program(s) that it is permitted to access and the library where the program(s) resides.

An associated GSO MAINT record will exist for each special user logonid, identifying the program(s) that it is permitted to access and the library where the

program(s) resides.

Example:

SET LID
CHANGE DFSMSHSM MAINT

CCI: CCI-002145

CCI: CCI-002883

CCI: CCI-003014

Group ID (Vulid): V-167

Group Title: ACF0670

Rule ID: SV-167r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0670](#)

Rule Title: There are GSO MAINT records that do not have corresponding maintenance LOGONIDs.

Vulnerability Discussion: LOGONIDs could be intentionally created that correspond to the GSO MAINT records. Then the maintenance programs could be used to gain unauthorized access to the system. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

- a) Display Resource Class Information as follows:
1. Logon to ACF2 and issue the following command:
LIST IF(MAINT)
 2. Press ENTER

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0670)
- b) If every GSO MAINT record has a corresponding maintenance logonid, there is NO FINDING.
- c) If any GSO MAINT record does not have a corresponding maintenance logonid, this is a FINDING.

Fix Text:

The IAO will ensure that an associated user logonid exists for each special GSO maintenance record identifying the program(s) that it is permitted to access and the library where the program(s) resides.

An associated GSO MAINT record will exist for each special user logonid, identifying the program(s) that it is permitted to access and the library where the program(s) resides.

Example:

SET LID
CHANGE DFSMSHSM MAINT

CCI: CCI-002145

CCI: CCI-002883

CCI: CCI-003014

Group ID (Vulid): V-2

Group Title: ACF0680

Rule ID: SV-2r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0680](#)

Rule Title: The LOGONIDs specified In GSO MAINT records will have the JOB and MAINT attributes specified In the associated LOGONID record.

Vulnerability Discussion: If there is a LOGONID intended for maintenance purposes that does not have the MAINT and JOB attributes specified, then it cannot function as intended. This could result in the inability to perform critical system maintenance tasks.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)
- ACF2CMDS.RPT(ATTMAINT)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0680)

1. Logon to ACF2 and issue the following command:

LIST IF(MAINT)

2. Press ENTER

For each logonid record associated to the LID entry in all GSO MAINT records specify the following, this is not a finding.

___ The JOB and MAINT attributes are specified.

Fix Text:

The IAO will ensure that logonids assigned to production maintenance tasks have the JOB and MAINT field settings in addition to the default LID field settings.

Production maintenance tasks manage the backups and restoration of data for the Continuity of Operations Plan (COOP) and media maintenance. Logonids assigned to production maintenance tasks will have the following field settings in addition to the default LID field settings:

JOB

MAINT

Example:

SET LID
CHANGE DFSMSHSM JOB MAINT

CCI: CCI-002145

CCI: CCI-002883

Group ID (Vulid): V-168
Group Title: ACF0690
Rule ID: SV-168r3_rule
Severity: CAT II
Rule Version (STIG-ID): [ACF0690](#)
Rule Title: Emergency LOGONIDs must be properly defined.

Vulnerability Discussion: Emergency USERIDs are necessary in the event of a system outage for recovery purposes. It is critical that those USERIDs be defined with the appropriate access to ensure timely restoration of services

Responsibility: Information Assurance Officer
IAControls: n/a

Check Content:

- a) Display USERIDs Information as follows:
1. a) Display Emergency LOGONIDs must be properly defined.:
 1. Logon to Administrator
 - 1 User Administration
 - 1 User Summary by Privilege
 - select ACCOUNT
- b) At a minimum an emergency logonid will exists with the security administration attributes specified in accordance with the following requirements:

For emergency IDs with security administration privileges, but which cannot access and update system data sets:

ACCOUNT

JCL
JOB

MONITOR
NONON CNCL
RULEVLD
RSRCVLD
SECURITY
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)

An additional class of usersids can exist to perform all operating system functions except ACP administration.

These emergency logonid / logonid(s) will have ability to access and update all system data sets, but will not have security administration privileges. See the following requirements:

JCL
JOB
MONITOR
NON CNCL (Will force logging of all activity.)
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)

All emergency logonid / logonid(s) are to be implemented with logging to provide an audit trail of their activities.

All emergency logonid / logonid(s) are to be maintained in both the ACP and SYS1.UADS to ensure they are available in the event that the ACP is not functional.

All emergency logonid / logonid(s) will have distinct, different passwords in SYS1.UADS and in the ACP, and the site is to establish procedures to ensure that the passwords differ. The password for any ID in SYS1.UADS is never to match the password for the same ID in the ACP.

All emergency logonid / logonid(s) will have documented procedures to provide a mechanism for the use of the IDs. Their release for use is to be logged, and the log is to be maintained by the ISSO. When an emergency logonid is released for use, its password is to be reset by the ISSO within 12 hours.

c) If all items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text:

Ensure that Emergency Logonids use these fields to enforce restrictions for Emergency Userids.

Two classes of emergency userids may exist. The following privileges and specifications will be used for these logonids:

Note: Only the emergency logonid with the security administration logonid attributes is required.

(1) For emergency IDs with the ability to access and update all system data sets, but which do not have security administration privileges:

```
NOFSRETAIN
JCL
JOB
MONITOR
NON CNCL (Will force logging of all activity.)
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)
```

Example:

```
SET LID
INSERT logonid NOFSRETAIN JCL JOB MONITOR NON-CNCL TSO TSOPRC(xxxxxxxx) TSOACCT(none)
```

(2) For emergency IDs with security administration privileges, but which cannot access and update system data sets:

```
ACCOUNT
NOFSRETAIN
JCL
JOB
MONITOR
NONON CNCL
RULEVLD
RSRCVLD
SECURITY
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)
```

Example:

SET LID

INSERT logonid ACCOUNT NOFSRETAIN JCL JOB MONITOR RULEVLD RSRCVLD NONON-CNCL SECURITY TSO TSOPRC(xxxxxxxx)
TSOACCT(none)

CCI: CCI-002145

CCI: CCI-002234

Group ID (Vulid): V-23

Group Title: ACF0710

Rule ID: SV-23r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0710](#)

Rule Title: The REFRESH attribute must be restricted.

Vulnerability Discussion: Unauthorized users may be able to effect changes to ACP system options. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

1. a) Display Emergency LOGONIDs must be properly defined.:

1. Logon to Administrator

L User Detail By LID Masking

Hit Enter

put a Y in REFRESH field and hit ENTER

Ensure the logonid with the REFRESH attribute is assigned to an IAO.

Fix Text:

The IAO will ensure Logonids with the refresh privilege are only available to IAOs and/or IAMs.

Ensure the logonid with the REFRESH attribute is assigned to an IAO.

Example:

SET LID
CHANGE logonid REFRESH

CCI: CCI-002145

CCI: CCI-002277

Group ID (Vulid): V-169

Group Title: ACF0720

Rule ID: SV-169r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0720](#)

Rule Title: LOGONIDS with the REFRESH attribute must have the SUSPEND attribute specified.

Vulnerability Discussion: Unauthorized users may be able to effect changes to ACP global system options. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

1. a) Display Emergency LOGONIDs must be properly defined.:

1. Logon to Administrator

L User Detail By LID Masking

Hit Enter

put a Y in REFRESH field and hit ENTER

Ensure that emergency logonids with the REFRESH attribute are in SUSPEND status.

Fix Text:

The IAO will ensure that logonids with the REFRESH attribute are in SUSPEND status unless actually in use.

The emergency logonids with the REFRESH attribute will be in SUSPEND status unless actually in use.

Example:

SET LID
CHANGE logonid SUSPEND

CCI: CCI-002145

CCI: CCI-002277

Group ID (Vulid): V-170

Group Title: ACF0730

Rule ID: SV-170r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0730](#)

Rule Title: There are no procedures to utilize the LOGONID with the REFRESH attribute.

Vulnerability Discussion: Individuals could effect unauthorized or inadvertent changes to ACP global system options. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

1. a) Display Emergency LOGONIDs must be properly defined.:

1. Logon to Administrator

L User Detail By LID Masking

Hit Enter

put a Y in REFRESH field and hit ENTER

b) If procedures exist in accordance with the STIG requirements to utilize the logonid with the REFRESH attribute to refresh ACF2 global options, there is NO FINDING.

Example:

When the IAO determines it necessary to refresh the ACF2 global options, the IAO will do the following:

1) Activate the REFRESH ID with the following setting(s):

NOSUSPEND
NOPSWD EXP
PASSWORD(new password)

2) Instruct Operations to perform the REFRESH.

3) Deactivate the REFRESH ID with the following setting:

SUSPEND

c) If no procedures exist in accordance with the STIG requirements to utilize the logonid with the REFRESH attribute to refresh ACF2 global options, this is a FINDING.

Fix Text:

The IAO will ensure procedures and documentation as defined below only exists for the use of Logonids with the refresh attribute.

Review security procedures for defining LOGONIDs and ensure documentation includes requirements for the LOGONID associated with the REFRESH attribute.

Example:

When the IAO determines it necessary to refresh the ACF2 global options, the IAO will do the following:

1) Activate the REFRESH ID with the following setting(s):

NOSUSPEND

NOPSWD EXP
PASSWORD(new password)

- 2) Instruct Operations to perform the REFRESH.
- 3) Deactivate the REFRESH ID with the following setting:

SUSPEND

CCI: CCI-000000

Group ID (Vulid): V-171

Group Title: ACF0750

Rule ID: SV-171r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0750](#)

Rule Title: LOGONIDs with the ACCOUNT, LEADER, or SECURITY attribute must be properly scoped.

Vulnerability Discussion: Individuals with these powerful attributes may have more extensive privileges than necessary to perform their job function. There could be no separation of duties and/or principle of least privilege in effect. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

1. a) Display Emergency LOGONIDs must be properly defined.:

1. Logon to Administrator

L User Detail By LID Masking

Hit Enter

Review all logonids for specific groups with the attributes ACCOUNT, LEADER, or SECURITY ensure they have the SCPLIST attribute specified properly according to job function and areas of responsibility.

NOTE: SCPLST attributes are not required for Domain Level Security Admin Logonids and BATCH Logonids that administer and modify the entire ACF2

environment to include GSO records, data set and resource rules, etc. or run audit reports.

Fix Text:

The IAO will ensure logonids with the ACCOUNT, LEADER, and SECURITY attributes are restricted by a SCPLIST attribute that restricts authority based on job function and area of responsibility.

The following user attributes allow update of the ACF2 databases for administering users, data set access rules, and Infostorage records. When granted to a logonid, restrict the scope of the following attributes using an associated SCPLIST (scope list) record:

ACCOUNT
LEADER
SECURITY

NOTE: SCPLST attributes are not required for Domain Level Security Admin Logonids and BATCH Logonids that administer and modify the entire ACF2 environment to include GSO records, data set and resource rules, etc. or run audit reports.

CCI: CCI-002227

CCI: CCI-002276

Group ID (Vulid): V-172

Group Title: ACF0760

Rule ID: SV-172r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0760](#)

Rule Title: There are LOGONIDs with the SECURITY attribute that do not have the RULEVLD and RSRCVLD attributes specified.

Vulnerability Discussion: Failure to assign the attribute bypasses security checking for the LOGONID and could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

1. a) Display LOGONIDs with SECURITY must be properly defined.:

1. Logon to Administrator

L User Detail By LID Masking

Hit Enter

Select SECRTY with Y and HIT ENTER

b) If all logonids with the SECURITY attribute also have the RULEVLD and RSRCVLD attributes specified, there is NO FINDING.

c) If any logonid with the SECURITY attribute does not have the RULEVLD and/or RSRCVLD attributes specified, this is a FINDING.

Fix Text:

The IAO will ensure Logonids with the SECURITY attribute have the RULEVLD and RSRCVLD attributes specified.

If a logonid is granted the SECURITY privilege, it is mandatory that RULEVLD and RSRCVLD attributes will also be specified for the logonid.

Example:

SET LID

CHANGE logonid RULEVLD RSRCVLD

CCI: CCI-000035

Group ID (Vulid): V-173

Group Title: ACF0770

Rule ID: SV-173r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0770](#)

Rule Title: The LOGONID with the ACCTPRIV attribute must be restricted to the IAO.

Vulnerability Discussion: Individuals with the ACCTPRIV could add or delete users in SYS1.UADS and jeopardize the availability of the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

1. a) Display LOGONIDs with SECURITY must be properly defined.:

b. Logon to ACF2

LIST IF(ACCTPRIV)

Hit Enter

Ensure that logonids with the ACCTPRIV attribute specified are assigned to the IAO.

Fix Text:

The IAO will ensure Logonids with the ACCTPRIV attribute are only reserved for use by the IAOs and/or IAMs.

The ACCTPRIV attribute cannot be scoped, and will be restricted exclusively to a site IAO:

Example:

SET LID

CHANGE logonid ACCTPRIV

CCI: CCI-000035

Group ID (Vulid): V-174

Group Title: ACF0780

Rule ID: SV-174r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0780](#)

Rule Title: The LOGONIDs with the AUDIT or CONSULT attribute must be properly scoped.

Vulnerability Discussion: Individuals with these attributes have the ability to view security definitions for resources not in their scope. This could result in the compromise of the confidentiality, integrity, and availability of the ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Display USERIDs Information as follows:

Ensure all logonids with the attributes AUDIT and/or CONSULT also have the SCPLIST attribute specified properly according to job function and areas of

responsibility.

NOTE: SCPLST attributes are not required for Logonids with the attributes AUDIT or CONSULT if the security IAM/IAO determines it requires ability to view the entire ACF2 environment. SCPLST attributes are not required for Auditors, Domain Level Security Admin Logonids, and BATCH Logonids that review the entire ACF2 environment to include GSO records, data set and resource rules, etc. or run audit reports.

1. a) logon to Administrator
1 User Summary by Privilege
- b. Logon to ACF2

Select AUDIT and/or CONSULT also have the SCPLIST attribute specified properly according to job function and areas of responsibility.

Fix Text:

The IAO will ensure that logonids with the AUDIT or CONSULT attributes are restricted by a SCPLIST attribute that restricts authority based on job function and area of responsibility.

The following user attributes allow viewing of the ACF2 databases for the purpose of inspecting users, data set access rules, and Infostorage records. When granted to a logonid, restrict the scope of the following attributes using an associated SCPLIST (scope list) record:

AUDIT
CONSULT

CCI: CCI-000035

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-175

Group Title: ACF0790

Rule ID: SV-175r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0790](#)

Rule Title: Procedures are not in place to ensure all LOGONIDs with the READALL attribute are used and controlled.

Vulnerability Discussion: READALL allows the individual to view any file and violates the principle of least privilege. This could result in the compromise of the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTREDAL)

1 Logon to Administrator

HIT ENTER

1 User Summary by Privilege

select READALL HIT ENTER

b) If procedures are in place to ensure logonids with the READALL attribute are used and controlled in accordance with the DISA requirements, there is NO FINDING.

c) If procedures are not in place to ensure logonids with the READALL attribute are used and controlled in accordance with the DISA requirements, this is a FINDING.

Fix Text:

The IAO will ensure that procedures are in place to control Logonids with the READALL attribute.

The READALL privilege is available for actual auditing of system data. It gives the capability of looking at every data set on the system despite the data set rules. Its use is strongly discouraged. Always grant access through the use of standard data set access rules. Under no circumstances will the privilege be used as a convenience to the person maintaining the rule sets. Only use this privilege when absolutely necessary, and only give it to auditors. Remove the privilege once the audit is complete. Fully document the granting and revoking of the access.

CCI: CCI-000035

CCI: CCI-000225

Group ID (Vulid): V-178

Group Title: ACF0820

Rule ID: SV-178r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0820](#)

Rule Title: The number of users granted the special privilege CONSOLE is not justified.

Vulnerability Discussion: Users with this privilege could intentionally or inadvertently issue console commands that could cause system resources and customer data to become unavailable.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTCONSL)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0820)

1. Logon to ACF2 and issue the following command:

LIST IF(CONSOLE)

2. Press ENTER

b) If the number of users granted the special privilege CONSOLE is strictly controlled (issued on an as-needed basis), there is NO FINDING.

c) If the number of users granted the special privilege CONSOLE is not strictly controlled (issued on an as-needed basis), this is a FINDING.

Fix Text:

The IAO will ensure that access to the CONSOLE attribute is kept to a minimum and is controlled and documented.

Review all LOGONIDs with the CONSOLE attribute.

Ensure documentation providing justification for access is maintained and filed with the IAO and that unjustified access is removed.

CCI: CCI-000213

CCI: CCI-000226

Group ID (Vulid): V-179

Group Title: ACF0830

Rule ID: SV-179r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0830](#)

Rule Title: The number of users granted the special privilege ALLCMDS is not justified.

Vulnerability Discussion: Users with this privilege may have access to restricted TSO commands and programs. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTALCMD)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0830)

1. Logon to ACF2 and issue the following command:

LIST IF(ALLCMDS)

2. Press ENTER

b) If the number of users granted the special privilege ALLCMDS is strictly controlled and access is granted on an as needed basis, there is NO FINDING.

c) If the number of users granted the special privilege ALLCMDS is not strictly controlled and access is granted on an as needed basis, this is a FINDING.

Fix Text:

The IAO will ensure that access to the special privilege ALLCMDS is kept to a minimum and is controlled and documented.

Review all LOGONIDs with the ALLCMDS attribute.

Ensure documentation providing justification for access is maintained and filed with the IAO and that unjustified access is removed.

CCI: CCI-000213

Group ID (Vulid): V-180

Group Title: ACF0840

Rule ID: SV-180r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ACF0840](#)

Rule Title: The number of users granted the special privilege PPGM is not justified.

Vulnerability Discussion: Users with this privilege may have access to powerful utilities and could intentionally or inadvertently compromise operating system integrity or destroy data on a large-scale basis. Misuse of these utilities could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTPPGM)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0840)

1. Logon to ACF2 and issue the following command:

LIST IF(PPGM)

2. Press ENTER

b) If the number of users granted the special privilege PPGM is strictly controlled and limited to systems programmer and operations personnel, there is NO FINDING.

c) If the number of users granted the special privilege PPGM is not strictly controlled and limited to systems programmer and operations personnel, this is a FINDING.

Fix Text:

The IAO will ensure that access to the special privilege PPGM is kept to a minimum and limited to systems programmer and operations personnel

Review all LOGONIDs with the PPGM attribute.

CCI: CCI-000213

Group ID (Vulid): V-181

Group Title: ACF0850

Rule ID: SV-00000r0_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0850](#)

Rule Title: The number of users granted the special privilege OPERATOR must be kept to a strictly controlled minimum.

Vulnerability Discussion: Users with this privilege can do anything from canceling jobs to disabling the entire system. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTOPER)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI(ACF0850)

1. Logon to ACF2 and issue the following command:

LIST IF(OPERATOR)

2. Press ENTER

If the number of users granted the special privilege "OPERATOR" is strictly controlled and limited to systems programmer and operations personnel, this is NOT a finding.

Security managers may be granted this access at the discretion of the ISSM.

If the number of users granted the special privilege "OPERATOR" is not strictly controlled and limited to systems programmer, security manager or operations personnel, this is a finding.

Fix Text:

Ensure that access to the special privilege "OPERATOR" is kept to a minimum and limited to systems programmer, security manager and operations personnel.

Review all LOGONIDs with the "OPERATOR" attribute.

CCI: CCI-000213

Group ID (Vulid): V-183

Group Title: ACF0870

Rule ID: SV-00000r0_rule

Severity: CAT II

Rule Version (STIG-ID): [ACF0870](#)

Rule Title: Sensitive Utility Controls will be properly defined and protected.

Vulnerability Discussion: Sensitive Utility Controls can run sensitive system privileges or controls, and potentially can circumvent system and security controls. Failure to properly control access to these resources could result in the compromise of the confidentiality, integrity, and availability of the operating system environment, system services, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ACF0870)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACF0870)

Ensure that all Sensitive Utilities resources and/or generic equivalent are properly protected according to the requirements specified in Sensitive Utility Controls table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

___ The ACF2 resources are defined with a default access of PREVENT.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel.

___ The ACF2 resource logging is correctly specified.

Fix Text:

The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Ensure that all Sensitive Utility Controls resources and/or generic equivalent are properly protected according to the requirements specified in Sensitive Utility Controls table in the z/OS STIG Addendum.

Use Sensitive Utility Controls table in the z/OS STIG Addendum. This table lists the resources, access requirements, and logging requirements for Sensitive Utilities, ensures the following guidelines are followed:

The ACF2 resources are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel.

The ACF2 resource logging is correctly specified.

The following commands are provided as a sample for implementing resource controls:

```
$KEY(AHLGTF) TYPE(PGM)
UID(stcgaudt) LOG
UID(*) PREVENT
```

```
F ACF2,REBUILD(PGM)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-108

Group Title: ACP00010

Rule ID: SV-108r2_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00010](#)

Rule Title: SYS1.PARMLIB is not limited to only system programmers.

Vulnerability Discussion: SYS1.PARMLIB contains the parameters which control system IPL, configuration characteristics, security facilities, and

performance. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(PARMRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00010)

___ The ACP data set rules for SYS1.PARMLIB allow inappropriate (e.g., global READ) access.

___ The ACP data set rules for SYS1.PARMLIB do not restrict READ, UPDATE and ALTER access to only systems programming personnel.

___ The ACP data set rules for SYS1.PARMLIB do not restrict READ and UPDATE access to only domain level security administrators.

___ The ACP data set rules for SYS1.PARMLIB do not restrict READ access to only system Level Started Tasks, authorized Data Center personnel, and auditors.

___ The ACP data set rules for SYS1.PARMLIB do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that update and alter access to SYS1.PARMLIB is limited to system programmers only and all update and alter access is logged.

Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required

The IAO will implement controls to specify the valid users authorized to update the SYS1.PARMLIB concatenation. All update and alter access to libraries in the concatenation will be logged using the ACP's facilities.

1. That systems programming personnel will be authorized to update and alter the SYS1.PARMLIB concatenation.

2. That domain level security administrators can be authorized to update the SYS1.PARMLIB concatenation.
3. That System Level Started Tasks, authorized Data Center personnel, and auditor can be authorized read access by the IAO.
4. That all update and alter access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-109

Group Title: ACP00020

Rule ID: SV-109r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00020](#)

Rule Title: Access to SYS1.LINKLIB is not properly protected.

Vulnerability Discussion: This data set is automatically APF-authorized, contains system SVCs and the base PPT. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(LINKRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00020)

___ The ACP data set rules for SYS1.LINKLIB allow inappropriate access.

___ The ACP data set rules for SYS1.LINKLIB do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for SYS1.LINKLIB do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged, this is a FINDING.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required. Under the ACPs SYS1.LINKLIB is always indicated as a program control library because it is a member of the MVS link list. Access is limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-110

Group Title: ACP00030

Rule ID: SV-110r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00030](#)

Rule Title: Write or greater access to SYS1.SVCLIB must be limited to system programmers only.

Vulnerability Discussion: This data set is automatically APF-authorized, contains system SVCs, and may also contain I/O appendages. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(SVCRPT)

Automated Analysis

Review the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00030)

___ Ensure that the ACP data set rules for SYS1.SVCLIB are limited to only appropriate authorized access.

___ Ensure that the ACP data set rules for SYS1.SVCLIB restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ Ensure that the ACP data set rules for SYS1.SVCLIB specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

Fix Text: The IAO must ensure that update and allocate access to SYS1.SVCLIB is limited to system programmers only and all update and allocate access is logged and reviewed. Periodic reviews of access authorization to critical system files must be performed. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes for SYS1.SVCLIB. SYS1.SVCLIB contains SVCs and I/O appendages as such: they are very powerful and will be strictly controlled to avoid compromising system integrity.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-111

Group Title: ACP00040

Rule ID: SV-111r4_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00040](#)

Rule Title: Write or greater access to SYS1.IMAGELIB must be limited to system programmers only.

Vulnerability Discussion: SYS1.IMAGELIB is a partitioned data set containing universal character set (UCS), forms control buffer (FCB), and printer control information. Most IBM standard UCS images are included in SYS1.IMAGELIB during system installation. This data set should be protected as a z/OS system data set.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(IMAGERPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection.

- PDI(ACP00040)

If the following guidance is true, this is not a finding.

___ The ACP data set rules for SYS1.IMAGELIB allow inappropriate access.

___ The ACP data set rules for SYS1.IMAGELIB do not restrict UPDATE and/or ALTER access to only systems programming personnel.

___ The ACP data set rules for SYS1.IMAGELIB do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

Fix Text: The IAO must ensure that UPDATE and/or ALLOCATE access to SYS1.IMAGELIB is limited to system programmers only and all update and allocate access is logged.

Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect SYS1.IMAGELIB.

SYS1.IMAGELIB is automatically APF-authorized. This data set contains modules, images, tables, and character sets which are essential to system print services.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-112

Group Title: ACP00050

Rule ID: SV-112r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00050](#)

Rule Title: Write or greater access to SYS1.LPALIB must be limited to system programmers only.

Vulnerability Discussion: SYS1.LPALIB is automatically APF-authorized during IPL processing and can contain SVCs. LPA modules, once loaded into the Link Pack Area, are capable of performing APF-authorized functions. This authorization allows a program to bypass various levels of security checking. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(LPARPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00050)

___ The ACP data set rules for SYS1.LPALIB allow inappropriate access.

___ The ACP data set rules for SYS1.LPALIB do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for SYS1.LPALIB do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect SYS1.LPALIB.

The IAO will ensure that update and allocate access to SYS1.LPALIB is limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Valid): V-113

Group Title: ACP00060

Rule ID: SV-113r2_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00060](#)

Rule Title: Update and allocate access to all APF -authorized libraries are not limited to system programmers only.

Vulnerability Discussion: The Authorized Program List designates those libraries that can contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(APFXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00060)

___ The ACP data set rules for APF libraries allow inappropriate access.

___ The ACP data set rules for APF libraries do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for APF libraries do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect APF Authorized Libraries.

The IAO will ensure that update and allocate access to all APF-authorized libraries are limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-108A

Group Title: ACP00062

Rule ID: SV-85847r1_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00062](#)

Rule Title: Libraries included in the system REXXLIB concatenation must be properly protected

Vulnerability Discussion: The libraries included in the system REXXLIB concatenation can contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(REXXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00062)

The ACP data set rules for libraries in the REXXLIB concatenation restrict inappropriate (e.g., GLOBAL read) access.

The ACP data set rules for libraries in the REXXLIB concatenation restrict WRITE or greater access to only z/OS systems programming personnel.
The ACP data set rules for libraries in the REXXLIB concatenation restrict READ access to the following:

Appropriate Started Tasks

Auditors

The user-id defined in PARMLIB member AXR00 AXRUSER(user-id)

The ACP data set rules for libraries in the REXXLIB concatenation specify that all (i.e., failures and successes) WRITE or greater access will be logged.

If all of the above are true, this is not a finding.

Fix Text: Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect APF Authorized Libraries.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-114

Group Title: ACP00070

Rule ID: SV-114r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00070](#)

Rule Title: Write or greater access to all LPA libraries must be limited to system programmers only.

Vulnerability Discussion: LPA modules, once loaded into the Link Pack Area, are capable of performing APF-authorized functions. This authorization allows a program to bypass various levels of security checking. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(LPAXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00070)

___ The ACP data set rules for LPA libraries allow inappropriate access.

___ The ACP data set rules for LPA libraries do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for LPA libraries do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect LPA Libraries.

The IAO will ensure that update and allocate access to all LPA libraries is limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-115

Group Title: ACP00080

Rule ID: SV-115r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00080](#)

Rule Title: Write or greater access to SYS1.NUCLEUS must be limited to system programmers only.

Vulnerability Discussion: This data set contains a large portion of the system initialization (IPL) programs and pointers to the master and alternate master catalog. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(NUCLRPT)

Automated Analysis

Refer to the following report produced by the a Data Set and Resource Data Collection:

- PDI(ACP00080)

___ The ACP data set rules for SYS1.NUCLEUS allow inappropriate access.

___ The ACP data set rules for SYS1.NUCLEUS do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for SYS1.NUCLEUS do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect SYS1.NUCLEUS.

The IAO will ensure that update and allocate access to SYS1.NUCLEUS is limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-116

Group Title: ACP00100

Rule ID: SV-116r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00100](#)

Rule Title: Write or greater access to libraries that contain PPT modules must be limited to system programmers only.

Vulnerability Discussion: Specific PPT designated program modules possess significant security bypass capabilities. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(PPTXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00100)

___ The ACP data set rules for libraries that contain PPT modules allow inappropriate access.

___ The ACP data set rules for libraries that contain PPT modules do not restrict UPDATE and ALLOCATE access to only z/OS systems programming personnel.

___ The ACP data set rules for libraries that contain PPT modules do not specify that all UPDATE and ALLOCATE access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect libraries containing modules listed in the Program Properties Table (PPT).

The IAO will ensure that update and allocate access to libraries containing PPT modules is limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-117

Group Title: ACP00110

Rule ID: SV-117r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00110](#)

Rule Title: Update and allocate access to LINKLIST libraries are not limited to system programmers only.

Vulnerability Discussion: The primary function of the LINKLIST is to serve as a single repository for commonly used system modules. Failure to ensure that the proper set of libraries are designated for LINKLIST can impact system integrity, performance, and functionality. For this reason, controls must be employed to ensure that the correct set of LINKLIST libraries are used. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(LNKXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00110)

___ The ACP data set rules for LINKLIST libraries allow inappropriate access.

___ The ACP data set rules for LINKLIST libraries do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for LINKLIST libraries do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

Note: Any DoD AIS Loadlibs defined to LINKLIST within z/OS Domains will be listed after all system libraiaies and will be removed on the test for access to systems programmers in the SRRAUDT check.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect the LINKLIST libraries.

The IAO will ensure that update and allocate access to LINKLIST libraries is limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-118

Group Title: ACP00120

Rule ID: SV-118r6_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00120](#)

Rule Title: The ACP security data sets and/or databases must be properly protected.

Vulnerability Discussion: The Access Control Program (ACP) database files contain all access control information for the operating system environment and system resources. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(ACPRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00120)

Verify that the accesses to the ACP security data sets and/or databases are properly restricted. If the following guidance is true, this is not a finding.

___ The ACP data set rules for ACP security data sets and/or databases restrict READ access to auditors and DASD batch.

___ The ACP data set rules for ACP security data sets and/or databases restrict READ and/or greater access to z/OS systems programming personnel, security personnel, and/or batch jobs that perform ACP maintenance.

___ All (i.e., failures and successes) data set access authorities (i.e. READ, UPDATE, ALTER, and CONTROL) for ACP security data sets and/or databases are logged.

Fix Text: Review access authorization to critical security database files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect the ACP Files.

Ensure that READ and/or greater access to all ACP files and/or databases are limited to system programmers and/or security personnel, and/or batch jobs that perform ACP maintenance. READ access can be given to auditors and DASD batch. All accesses to ACP files and/or databases are logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

CCI: CCI-002357

Group ID (Vulid): V-119

Group Title: ACP00130

Rule ID: SV-119r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00130](#)

Rule Title: Access greater than Read to the System Master Catalog must be limited to system programmers only.

Vulnerability Discussion: System catalogs are the basis for locating all files on the system. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(CATMRPT) - Master Catalog

Automated Analysis:

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00130)

If data set rules for System catalogs allow inappropriate access, this is a finding.

If data set rules for the Master Catalog do not restrict greater than READ access to only z/OS systems programming personnel, this is a finding.

Access greater than READ for the Master catalog is allowed to a batch job ID in the following specific case:

The batch job must reside in a data set that is restricted to systems programmers only.

If dataset rules for the Master Catalog do not specify that all (i.e., failures and successes) greater than READ access will be logged, this is a finding.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect the MASTER CATALOG.

The IAO will ensure that greater than READ access to MASTER CATALOG is limited to system programmers only and all greater than READ access is logged.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-4850

Group Title: ACP00135

Rule ID: SV-4850r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00135](#)

Rule Title: Allocate access to system user catalogs must be limited to system programmers only.

Vulnerability Discussion: System catalogs are the basis for locating all files on the system. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(CATURPT) - User Catalogs

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00135)

___ The ESM data set rules for System Catalogs allow inappropriate access.

___ The ESM data set rules for User Catalogs do not restrict ALTER access / ALTER and SCRATCH (TSS) to only z/OS systems programming personnel. Access greater than READ for User Catalog is allowed to a batch job ID in the following specific case:
The batch job must reside in a data set that is restricted to systems programmers only.

___ The ESM data set rules for User Catalogs do not specify that all (i.e., failures and successes) ALTER access will be logged.

- b) If all of the above are untrue, this is not a finding.
- c) If any of the above is true, this is a finding.

Fix Text: Review access authorization to critical system files.

Evaluate the impact of correcting the deficiency.

Develop a plan of action and implement the changes as required to protect USER CATALOGS.

Configure ESM rules for allocate access to USER CATALOGS, limited to system programmers only, and all allocate access is logged.

Configure ESM rules for the USER CATALOGS to allow any batch ID access above READ only in this specific case: The batch job that requires above READ access must reside in a data set that has restricted ALTER or equivalent access to systems programmers ONLY.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-120

Group Title: ACP00140

Rule ID: SV-120r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00140](#)

Rule Title: Update and allocate access to all system-level product installation libraries are not limited to system programmers only.

Vulnerability Discussion: System-level product installation libraries constitute the majority of the systems software libraries. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(SMPERPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00140)

Have the systems programmer for z/OS supply the following information:

- The data set name and associated SREL for each SMP/E CSI utilized to maintain this system.
- The data set name of all SMP/E TLIBs and DLIBs used for installation and production support. A comprehensive list of the SMP/E DDDEFs for all CSIs may be used if valid.

___ The ACP data set rules for system-level product installation libraries (e.g., SMP/E CSIs) allow inappropriate access.

___ The ACP data set rules for system-level product installation libraries (e.g., SMP/E CSIs) do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, or if these data sets cannot be identified due to a lack of requested information, this is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect System-level product installation libraries,

The IAO will ensure that update and allocate access to all system-level product execution libraries are limited to system programmers only.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-121

Group Title: ACP00150

Rule ID: SV-121r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00150](#)

Rule Title: Update and allocate access to the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) are not limited to system programmers only.

Vulnerability Discussion: The JES2 System data sets are a common repository for all jobs submitted to the system and the associated printout and configuration of the JES2 environment. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(JES2RPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00150)

___ The ACP data set rules for the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) allow inappropriate access.

___ The ACP data set rules for the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) do not restrict UPDATE and/or ALTER access to only z/OS systems programming personnel.

b) If both of the above are untrue, there is NO FINDING.

c) If either of the above is true, this is a FINDING.

Fix Text: Limit read and write access to the JES2 started task. Limit allocate/alter access to the systems programming staff. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect JES2 System datasets (spool, checkpoint, and parmlib datasets)

The IAO will ensure that update and allocate access to JES2 System datasets (spool, checkpoint, and parmlib datasets) are limited to system programmers only. For example all SYS1.HASP* data sets.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-122

Group Title: ACP00170

Rule ID: SV-122r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00170](#)

Rule Title: Write or greater access to SYS1.UADS must be limited to system programmers only and read and update access must be limited to system programmer personnel and/or security personnel.

Vulnerability Discussion: SYS1.UADS is the data set where emergency USERIDs are maintained. This ensures that logon processing can occur even if the ACP is not functional. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(UADSRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00170)

___ The ACP data set rules for SYS1.UADS allow inappropriate access.

___ The ACP data set rules for SYS1.UADS do not restrict ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for SYS1.UADS do not restrict READ and/or UPDATE access to z/OS systems programming personnel and/or security personnel.

____ The ACP data set rules for SYS1.UADS do not specify that all (i.e., failures and successes) data set access authorities (i.e., READ, UPDATE, ALTER, and CONTROL) will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: SYS1.UADS allocate/alter authority is limited to the systems programming staff. Read and update access should be limited to the security staff. Evaluate the impact of correcting any deficiency. Develop a plan of action and implement the changes as required to protect SYS1.UADS.

The IAO will ensure that allocate access to SYS1.UADS is limited to system programmers only, read and update access to SYS1.UADS is limited to system programmer personnel and/or security personnel and all dataset access is logged.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-123

Group Title: ACP00180

Rule ID: SV-123r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00180](#)

Rule Title: Update and allocate access to SMF collection files (i.e., SYS1.MANx) are not limited to system programmers and/or batch jobs that perform SMF dump processing.

Vulnerability Discussion: SMF data collection is the system activity journaling facility of the z/OS system. With the proper parameter designations it serves as the basis to ensure individual user accountability. SMF data is the primary source for cost charge back in DISA. Unauthorized access could result in the compromise of logging and recording of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(SMFXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00180)

___ The ACP data set rules for the SMF data collection files (e.g., SYS1.MAN*) allow inappropriate access.

___ The ACP data set rules for the SMF data collection files (e.g., SYS1.MAN*) do not restrict ALTER access to only z/OS systems programming personnel.

___ The ACP data set rules for the SMF data collection files (e.g., SYS1.MAN*) do not restrict UPDATE access to z/OS systems programming personnel, and/or batch jobs that perform SMF dump processing.

___ The ACP data set rules for SMF data collection files (e.g., SYS1.MAN*) do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect modification or deletion of SMF collection files.

The IAO will ensure that allocate/alter authority to SMF collection files is limited to only systems programming staff and and/or batch jobs that perform SMF dump processing and ensure the accesses are being logged.

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-124

Group Title: ACP00190

Rule ID: SV-124r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00190](#)

Rule Title: Update and allocate access to data sets used to backup and/or dump SMF collection files are not limited to system programmers and/or batch jobs that perform SMF dump processing.

Vulnerability Discussion: SMF backup data sets are those data sets to which SMF data has been offloaded in order to ensure a historical tracking of individual user accountability. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(SMFBKRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00190)

Have the systems programmer supply the procedures and collection specifics for SMF datasets and backup.

___ The ACP data set rules for the SMF dump/backup files allow inappropriate access.

___ The ACP data set rules for the SMF dump/backup files do not restrict UPDATE and/or ALTER access to authorized DISA and site personnel (e.g., systems programmers and batch jobs that perform SMF processing).

___ The ACP data set rules for SMF dump/backup files do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, or if these data sets cannot be identified due to a lack of requested information, this is a FINDING.

Fix Text: The IAO will ensure that update and allocate access to datasets used to backup and/or dump SMF collection files is limited to system programmers and/or batch jobs that perform SMF dump processing and all dataset access is logged.

Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect datasets used to backup and/or dump SMF Collection Files.

In z/OS systems, SMF data is the ultimate record of system activity. Therefore, SMF data is of the most sensitive and critical nature. While the length of time for which SMF data will be retained is not specifically regulated, it is imperative that the information is available for the longest possible time period in case of subsequent investigations. The statute of limitations varies according to the nature of a crime. It may vary by jurisdiction, and some crimes are not subject to a statute of limitations. Apply the following guidelines to the retention of SMF data for all DOD systems:

(a) Retain at least two (2) copies of the SMF data.

(b) Maintain SMF data for a minimum of one year.

(c) All update and alter access authority to SMF history files will be logged using the ACP's facilities. Only systems programming personnel and batch jobs that perform SMF functions will be authorized to update the SMF files.

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-125

Group Title: ACP00200

Rule ID: SV-125r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00200](#)

Rule Title: Access to SYSTEM DUMP data sets are not limited to system programmers only.

Vulnerability Discussion: System DUMP data sets are used to record system data areas and virtual storage associated with system task failures. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(DUMPRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00200)

___ The ACP data set rules for System Dump data sets allow inappropriate access.

___ The ACP data set rules for System Dump data sets do not restrict READ, UPDATE and/or ALTER access to only systems programming personnel.

___ The ACP data set rules for all System Dump data sets do not restrict READ access to personnel having justification to review these dump data sets for debugging proposes.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

The dump data sets displayed by the DD command along with the dump datasets specified in the DUMPSRV routine are to be restricted to system programmers unless unless a letter justifying access is filed with the IAO.

Fix Text: The IAO will ensure that access to SYSTEM DUMP data set(s) is limited to system programmers only, unless a letter justifying access is filed with the IAO.

Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to restrict access to these data sets.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-126

Group Title: ACP00210

Rule ID: SV-126r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00210](#)

Rule Title: Update and allocate access to System backup files are not limited to system programmers and/or batch jobs that perform DASD backups.

Vulnerability Discussion: System backup data sets are necessary for recovery of DASD resident data sets. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: CODB-1, DCCS-1, DCCS-2, ECCD-1

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(BKUPRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00210)

Collect from the storage management group the identification of the DASD backup files and all associated storage management userids/LIDs/ACIDs.

___ The ACP data set rules for system DASD backup files allow inappropriate access.

___ The ACP data set rules for system DASD backup files do not restrict UPDATE and ALLOCATE access to z/OS systems programming and/or batch jobs

that perform DASD backups.

- b) If both of the above are untrue, there is NO FINDING.
- c) If either of the above is true, or if these data sets cannot be identified due to a lack of requested information, this is a FINDING.

Fix Text: Obtain the high level indexes to backup datasets names and verify that their access is restricted by the System's ACP to System Programmers and batch jobs that perform the backups. If any other userids are specified, make sure that the IAO has documented justification for the access.

CCI: CCI-000213

Group ID (Vulid): V-127

Group Title: ACP00220

Rule ID: SV-127r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00220](#)

Rule Title: Access to SYS(x).TRACE is not limited to system programmers only.

Vulnerability Discussion: SYS1.TRACE is used to trace and debug system problems. Unauthorized access could result in a compromise of the integrity and availability of all system data and processes.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

- a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(TRACERPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00220)

___ The ACP data set rule for SYS1.TRACE allows inappropriate access.

___ The ACP data set rule for SYS1.TRACE does not restrict access to systems programming personnel and started tasks that perform GTF processing.

- b) If both of the above are untrue, there is NO FINDING.
- c) If either of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that access to SYS1.TRACE is limited to system programmers only.

CCI: CCI-000213

Group ID (Vulid): V-128

Group Title: ACP00230

Rule ID: SV-128r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00230](#)

Rule Title: Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) are not limited to system programmers.

Vulnerability Discussion: Page data sets hold individual pages of virtual storage when they are paged out of real storage. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(PGXXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00230)

___ The ACP data set rules for system page data sets (PLPA, COMMON, and LOCAL) allow inappropriate access.

___ The ACP data set rules for system page data sets (PLPA, COMMON, and LOCAL) do not restrict access to only systems programming personnel.

- b) If both of the above are untrue, there is NO FINDING.

c) If either of the above is true, this is a FINDING

Fix Text: Verify that the ACP data set rules for system page data sets (PLPA, COMMON, and LOCAL) restrict access to only systems programming personnel.

CCI: CCI-000213

Group ID (Vulid): V-129

Group Title: ACP00240

Rule ID: SV-129r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00240](#)

Rule Title: Write or greater access to Libraries containing EXIT modules must be limited to system programmers only.

Vulnerability Discussion: System exits have a wide range of uses and capabilities within any system. Exits may introduce security exposures within the system, modify audit trails, and alter individual user capabilities. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(MVSXRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00240)

___ The ACP data set rules for libraries that contain exit modules allow inappropriate access.

___ The ACP data set rules for libraries that contain system exit modules do not restrict UPDATE and ALLOCATE access to only z/OS systems programming personnel.

___ The ACP data set rules for libraries that contain exit modules do not specify that all UPDATE and ALLOCATE access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Using the ACP, protect the data sets associated with all product exits installed in the z/OS environment. This reduces the potential of a hacker adding a routine to a library and possibly creating an exposure. See that all exits are tracked using a CMP. Develop usermods to include the source/object code used to support the exits. Have Systems programming personnel review all z/OS and other product exits to confirm that the exits are required and are correctly installed.

Have the IAO validate that all update and alter access to libraries containing z/OS and other system level exits will be logged using the ACP s facilities. Only systems programming personnel will be authorized to update the libraries containing z/OS and other system level exits.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-234

Group Title: ACP00250

Rule ID: SV-234r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00250](#)

Rule Title: All system PROCLIB data sets must be limited to system programmers only

Vulnerability Discussion: Unauthorized access to PROCLIB data sets referenced in the JES2 procedure can allow unauthorized modifications to STCs and other system level procedures. This could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(PROCRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00250)

Refer to the following for the PROCLIB data sets that contain the STCs and TSO logons from the following sources:

- MSTJCLxx member used during an IPL. The PROCLIB data sets are obtained from the IEFPSI and IEFJOBS DD statements.
- PROCxx DD statements and JES2 Dynamic PROCLIBs. Where xx is the PROCLIB entries for the STC and TSU JOBCLASS configuration definitions.

Verify that the accesses to the above PROCLIB data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The ACP data set access authorizations restrict READ access to all authorized users.

___ The ACP data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

Fix Text: The IAO will ensure that all WRITE and/or greater access to all PROCLIBs referenced in the Master JCL and JES2 or JES3 procedure for started tasks (STCs) and TSO logons are restricted to systems programming personnel only.

Suggestion on how to update system to be compliant with this vulnerability:

NOTE: All examples are only examples and may not reflect your operating environment.

Obtain only the PROCLIB data sets that contain STC and TSO procedures. The data sets to be reviewed are obtained using the following steps:

- All data sets contained in the MSTJCLxx member in the DD statement concatenation for IEFPSI and IEFJOBS.
- The data set in the PROCxx DD statement concatenation that are within the JES2 procedure or identified in the JES2 dynamic PROCLIB definitions. The specific PROCxx DD statement that is used is obtained from the PROCLIB entry for the JOBCLASSES of STC and TSU. The following is what data sets the process will obtain for analysis:

MSTJCL00

```
//MSTJCL00 JOB MSGLEVEL=(1,1),TIME=1440
// EXEC PGM=IEEMB860,DPRTY=(15,15)
//STCINRDR DD SYSOUT=(A,INTRDR)
//TSOINRDR DD SYSOUT=(A,INTRDR)
//IEFPDSI DD DSN=SYS3.PROCLIB,DISP=SHR <<===
// DD DSN=SYS2.PROCLIB,DISP=SHR <<===
// DD DSN=SYS1.PROCLIB,DISP=SHR <<===
//SYSUADS DD DSN=SYS1.UADS,DISP=SHR
```



```
//SYSLBC DD DSN=SYS1.BROADCAST,DISP=SHR
```

JES2

```
//JES2 PROC
//IEFPROC EXEC PGM=HASJES20,PARM=NOREQ,
// DPRTY=(15,15),TIME=1440,PERFORM=9
//ALTPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2BKUP)
//HASPPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2PARM)
//PROC00 DD DSN=SYS3.PROCLIB,DISP=SHR <<===
// DD DSN=SYS2.PROCLIB,DISP=SHR <<===
// DD DSN=SYS1.PROCLIB,DISP=SHR <<===
//PROC01 DD DSN=SYS4.USERPROC,DISP=SHR
// DD DSN=SYS3.PROCLIB,DISP=SHR
// DD DSN=SYS2.PROCLIB,DISP=SHR
// DD DSN=SYS1.PROCLIB,DISP=SHR
//IEFRDER DD SYSOUT=*
//HASPLIST DD DDNAME=IEFRDER
```

JES2 initialization parameter JOBCLASS PROCLIB entries

```
JOBCLASS(*) ACCT=NO, /* ACCT # NOT REQUIRED (DEF.)*/
```

```
PROCLIB=01, /* DEFAULT TO //PROC01 DD (DEF.)*/
```

```
JOBCLASS(STC) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/
```

```
PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
```

```
JOBCLASS(TSU) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/
```

```
PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
```

PROCLIB data set that will be used in the access authorization process:

```
SYS3.PROCLIB
SYS2.PROCLIB
```

SYS1.PROCLIB

The following PROCLIB data set will NOT be used or evaluated:

SYS4.USERPROC

Recommendation for sites:

The following are recommendations for the sites to ensure only PROCLIB data sets that contain the STC and TSO procedures are protected.

- Remove all application PROCLIB data sets from MSTJCLxx and JES2 procedures. The customer will have all JCL changed to use the JCLLIB JCL statement to refer to the application PROCLIB data sets.

Example:

```
//USERPROC JCLLIB ORDER=(SYS4.USERPROC)
```

- Remove all access to the application PROCLIB data sets and only authorize system programming personnel WRITE and/or greater access to these data sets.
- Document the application PROCLIB data set access for the customers that require WRITE and/or greater access. Use this documentation as justification for the inappropriate access created by the scripts.
- Change MSTJCLxx and JES2 procedure to identify STC and TSO PROCLIB data sets separate from application PROCLIB data sets. The following is a list of actions that can be performed to accomplish this recommendation:
 - a. Ensure that MSTJCLxx contains only PROCLIB data sets that contain STC and TSO procedures.
 - b. If an application PROCLIB data set is required for JES2, ensure that the JES2 procedure specifies more than one PROCxx DD statement concatenation or identified in the JES2 dynamic PROCLIB definitions. Identify one PROCxx DD statement data set concatenation that contains the STC and TSO PROCLIB data sets. Identify one or more additional PROCxx DD statements that can contain any other PROCLIB data sets. The concatenation of the additional PROCxx DD statements can contain the same data sets that are identified in the PROCxx DD statement for STC and TSO. The following is an example of the JES2 procedure:

```
//JES2 PROC
//IEFPROC EXEC PGM=HASJES20,PARM=NOREQ,
// DPRTY=(15,15),TIME=1440,PERFORM=9
//ALTPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2BKUP)
//HASPPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2PARM)
//PROC00 DD DSN=SYS3.PROCLIB,DISP=SHR
// DD DSN=SYS2.PROCLIB,DISP=SHR
```

```
// DD DSN=SYS1.PROCLIB,DISP=SHR
//PROC01 DD DSN=SYS4.USERPROC,DISP=SHR
// DD DSN=SYS3.PROCLIB,DISP=SHR
// DD DSN=SYS2.PROCLIB,DISP=SHR
// DD DSN=SYS1.PROCLIB,DISP=SHR
//IEFRDER DD SYSOUT=*
//HASPLIST DD DDNAME=IEFRDER
```

c. Ensure that the JES2 configuration file is changed to specify that the PROCLIB entry for the STC and TSU JOBCLASSES point to the proper PROCxx entry within the JES2 procedure or JES2 dynamic PROCLIB definitions that contain the STC and/or TSO procedures. All other JOBCLASSES can specify a PROCLIB entry that uses the same PROCxx or any other PROCxx DD statement identified in the JES2 procedure or identified in the JES2 dynamic PROCLIB definitions. The following is an example of the JES2 initialization parameters:

```
JOBCLASS(*) ACCT=NO, /* ACCT # NOT REQUIRED (DEF.)*/

PROCLIB=01, /* DEFAULT TO //PROC01 DD (DEF.)*/

JOBCLASS(STC) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/

PROCLIB=00, /* USE //PROC00 DD (DEF.)*/

JOBCLASS(TSU) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/

PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
```

d. Ensure that only system programming personnel are authorized WRITE and/or greater access to PROCLIB data sets that contain STC and TSO procedures.

CCI: CCI-000213

Group ID (Vulid): V-182

Group Title: ACP00260

Rule ID: SV-31711r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00260](#)

Rule Title: Memory and privileged program dumps must be protected in accordance with proper security requirements.

Vulnerability Discussion: Access to memory and privileged program dumps running Trusted Control Block (TCB) key 0-7 may hold passwords, encryption keys, or other sensitive data that must not be made available. Failure to properly control access to these facilities could result in unauthorized personnel modifying sensitive z/OS lists. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

From a command input screen enter:

SET RESOURCE (FAC)

SET VERBOSE

LIST LIKE (IEAABD-)

Alternately, this can be viewed by following steps:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ACP00260)

- ACF2CMDS.RPT(RESOURCE) Alternate report

NOTE: If CLASMAP defines FACILITY as anything other than the default of TYPE(FAC), replace FAC with the appropriate three letters.

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00260)

Ensure that the Memory and privileged program dumps resources are properly protected as stated below. If all of the following guidance is true, this is not a finding.

___ Ensure that the IEAABD. resource and/or generic equivalent is defined with PREVENT access and that access is not available to any user.

___ Ensure that IEAABD.DMPAUTH. resource and/or generic equivalent is defined and access with SERVICE(READ) is limited to authorized users that have a valid job duties requirement for access.

___ Ensure that IEAABD.DMPAUTH. resource and/or generic equivalent is defined and access with the SERVICE(UPDATE) or greater is restricted to only systems personnel and that all access is logged.

___ Ensure that IEAABD.DMPAKEY. resource and/or generic equivalent is defined and all access is restricted to systems personnel and that all access is logged.

Fix Text: Memory and privileged program dump resources are provided via resources in the FACILITY resource class. Ensure that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product s installation guide and can be site specific.)

Below is listed the access requirements for memory and privileged program dump resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent are followed. When protecting the facilities for dumps lists via the FACILITY resource class, ensure that the following items are in effect:

IEAABD.
IEAABD.DMPAUTH.
IEAABD.DMPAKEY.

The ACF2 resources are defined with a default access of PREVENT.

Ensure that no access is given to IEAABD. resource.

Example:

```
$KEY(IEAABD) TYPE(FAC)  
- UID(*) PREVENT
```

IEAABD.DMPAUTH. READ access is limited to authorized users that have a valid job duties requirement for access. UPDATE access will be restricted to system programming personnel and access will be logged.

Example:

```
$KEY(IEAABD) TYPE(FAC)  
DMPAUTH.- UID(syspautd) SERVICE(UPDATE) LOG  
DMPAUTH.- UID(authusers) SERVICE(READ)  
DMPAUTH.- UID(*) PREVENT
```

IEAABD.DMPAKEY. access will be restricted to system programming personnel and access will be logged.

Example:

\$KEY(IEAABD) TYPE(FAC)
DMPAKEY.- UID(syspautd) LOG
DMPAKEY.- UID(*) PREVENT

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-36

Group Title: ACP00270

Rule ID: SV-6409r8_rule

Severity: CAT I

Rule Version (STIG-ID): [ACP00270](#)

Rule Title: Dynamic lists must be protected in accordance with proper security requirements.

Vulnerability Discussion: Dynamic lists provide a method of making z/OS system changes without interrupting the availability of the operating system. Failure to properly control access to these facilities could result in unauthorized personnel modifying sensitive z/OS lists. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Systems Programmer

IAControls: N/A

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(FACILITY)
- ACF2CMDSD.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00270)

Verify that the accesses for CSV-prefixed resources are properly restricted. If the following guidance is true, this is not a finding.

___ The ACF2 resources and/or generic equivalent are defined with a default access of PREVENT.

___ The ACF2 resources and/or generic equivalent identified below will be defined with LOG and SERVICE(UPDATE) access restricted to system programming personnel:

CSVAPF.
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.
CSVDYNEX.
CSVDYNEX.LIST
CSVDYNL.
CSVDYNL.UPDATE.LNKLIST
CSVLLA.

___ The ACF2 CSVDYNEX.LIST resource and/or generic equivalent will be defined with LOG and SERVICE(UPDATE) access restricted to system programming personnel.

___ The ACF2 CSVDYNEX.LIST resource and/or generic equivalent will be defined with SERVICE(READ) access restricted to auditors.

___ If the products CICS and/or CONTROL-O are on the system, the ACF2 access to the CSVLLA resource and/or generic equivalent will be defined with LOG and SERVICE(UPDATE) access restricted to the CICS and CONTROL-O STC logonids.

___ If any software product requires access to dynamic LPA updates on the system, the ACF2 access to the CSVDYLPA resource and/or generic equivalent will be defined with AUDIT(ALL) and UPDATE only after the product has been validated with the appropriate STIG or SRG for compliance AND receives documented and filed authorization that details the need and any accepted risks from the site ISSM or equivalent security authority.

Note: In the above, SERVICE(UPDATE) can be substituted with ADD, CONTROL, or LOG/ALLOW. Review the rules definitions in the ACF2 documentation when specifying SERVICE(UPDATE).

Fix Text: Ensure that the Dynamic List resources are defined to the FACILITY resource class and protected. Only system programmers and a limited number of authorized users and Approved authorized Started Tasks are able to issue these commands. All access is logged.

The required CSV-prefixed Facility Class resources are listed below. These resources or generic equivalents should be defined and permitted as required with only z/OS systems programmers and logging enabled. Minimum required list of CSV-prefixed resources:

CSVAPF.**
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.**

CSV DY LPA.ADD.**
CSV DY LPA.DELETE.**
CSV DY NEX.**
CSV DY NEX.LIST
CSV DY NL.**
CSV DY NL.UPDATE.LNK LST
CSV LLA.**

Limit authority to those resources to z/OS systems programmers. Restrict to the absolute minimum number of personnel with AUDIT(ALL(READ)) and UPDATE access.

Sample commands are shown here to accomplish this:

RDEF FACILITY CSV APF.** UACC(NONE) OWNER(syspau dt) AUDIT(ALL(READ))
RDEF FACILITY CSV APF.MVS.SETPROG.FORMAT.DYNAMIC.** UACC(NONE) OWNER(syspau dt) AUDIT(ALL(READ))
RDEF FACILITY CSV APF.MVS.SETPROG.FORMAT.STATIC.** UACC(NONE) OWNER(syspau dt) AUDIT(ALL(READ))

PERMIT CSV APF.** CLASS(FACILITY) ID(syspau dt) ACCESS(UPDATE)
PERMIT CSV APF.MVS.SETPROG.SETPROG.FORMAT.DYNAMIC.** CLASS(FACILITY) ID(syspau dt) ACCESS(UPDATE)
PERMIT CSV APF.MVS.SETPROG.SETPROG.FORMAT.STATIC.** CLASS(FACILITY) ID(syspau dt) ACCESS(UPDATE)

The CSV DY LPA.ADD resource will be permitted to products BMC Mainview, CA 1, and CA Common Services STC userids with AUDIT(ALL(READ)) and UPDATE access.

The CSV DY LPA.DELETE resource will be permitted to products CA 1 and CA Common Services STC userids with AUDIT(ALL(READ)) and UPDATE access.

Sample commands are shown here to accomplish one set of resources:

RDEF FACILITY CSV DY LPA.** UACC(NONE) OWNER(syspau dt) AUDIT(ALL(READ))
RDEF FACILITY CSV DY LPA.ADD.** UACC(NONE) OWNER(syspau dt) AUDIT(ALL(READ))
RDEF FACILITY CSV DY LPA.DELETE.** UACC(NONE) OWNER(syspau dt) AUDIT(ALL(READ))

PERMIT CSV DY LPA.** CLASS(FACILITY) ID(syspau dt) ACCESS(UPDATE)
PERMIT CSV DY LPA.** CLASS(FACILITY) ID(BMC Mainview STC userid) ACCESS(UPDATE)
PERMIT CSV DY LPA.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)
PERMIT CSV DY LPA.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
PERMIT CSV DY LPA.ADD.** CLASS(FACILITY) ID(syspau dt) ACCESS(UPDATE)
PERMIT CSV DY LPA.ADD.** CLASS(FACILITY) ID(BMC Mainview STC userid) ACCESS(UPDATE)
PERMIT CSV DY LPA.ADD.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)


```
PERMIT CSV DY LPA.ADD.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
PERMIT CSV DY LPA.DELETE.** CLASS(FACILITY) ID(sy spaudt) ACCESS(UPDATE)
PERMIT CSV DY LPA.DELETE.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)
PERMIT CSV DY LPA.DELETE.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
```

The CSV DY NEX.LIST resource and/or generic equivalent will be defined with AUDIT(FAILURE(READ)SUCCESS(UPDATE)) and UPDATE access restricted to system programming personnel.

The CSV DY NEX.LIST resource and/or generic equivalent will be defined with READ access restricted to auditors.

Sample commands are shown here to accomplish this:

```
RDEF FACILITY CSV DY NEX.** UACC(NONE) OWNER(sy spaudt)
AUDIT(ALL(READ))
RDEF FACILITY CSV DY NEX.LIST.** UACC(NONE) OWNER(sy spaudt)
AUDIT(FAILURE(READ)SUCCESS(UPDATE))
```

```
PERMIT CSV DY NEX.** CLASS(FACILITY) ID(sy spaudt) ACCESS(UPDATE)
PERMIT CSV DY NEX.LIST.** CLASS(FACILITY) ID(sy spaudt) ACCESS(UPDATE)
PERMIT CSV DY NEX.LIST.** CLASS(FACILITY) ID(audtaudt) ACCESS(READ)
```

The CSV LLA resource will be permitted to CICS and CONTROL-O STC userids with AUDIT(ALL(READ)) and UPDATE access.

Sample commands are shown here to accomplish one set of resources:

```
RDEF FACILITY CSV LLA.** UACC(NONE) OWNER(sy spaudt) AUDIT(ALL(READ))

PERMIT CSV LLA.** CLASS(FACILITY) ID(sy spaudt) ACCESS(UPDATE)
PERMIT CSV LLA.** CLASS(FACILITY) ID(CICS STC userids) ACCESS(UPDATE)
PERMIT CSV LLA.** CLASS(FACILITY) ID(CONTROL-O STC userid) ACCESS(UPDATE)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-7482

Group Title: ACP00282

Rule ID: SV-7919r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00282](#)

Rule Title: z/OS system commands must be properly protected.

Vulnerability Discussion: z/OS system commands provide a method of controlling the operating environment. Failure to properly control access to z/OS system commands could result in unauthorized personnel issuing sensitive system commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

From a command screen enter:

SET RESOURCE (OPR)

SET VERBOSE

LIST LIKE (-)

NOTE: If CLASMAP defines OPERCMDS as anything other than the default of TYPE(OPR), replace OPR with the appropriate three letters.

Alternately:

Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(ACP00282)
- SENSITVE.RPT(OPERCMDS) - Alternate report
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00282)

The MVS resource is defined to the OPERCMDS class with a default access of PREVENT, and all access logged, i.e., MVS.** is defined with access of PREVENT

Access to z/OS system commands defined in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum, is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

Access to specific z/OS system commands is logged as indicated in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum.

If any of the above is untrue for any z/OS system command resource, this is a FINDING.

If all of the above are true, there is NO FINDING.

Fix Text: z/OS system commands provide control over z/OS functions and can compromise security if misused. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the z/OS system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when all less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

Apply the following recommendations when implementing security:

The MVS.** resource is defined to the OPERCMDS class with an access of NONE and all (i.e., failures and successes) access logged.

Access to z/OS system commands defined in the "Required Controls on z/OS System Commands" table in the zOS STIG Addendum is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

All access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled "Required Controls on z/OS System Commands" in the zOS STIG Addendum.

A sample set of commands to define and permit access to system command resources is shown here:

```
RDEF OPERCMDS MVS.** UACC(NONE) OWNER(<sypaudt>) AUDIT(ALL(READ)) DATA("set up deny-by-default profile per srr pdi acp00282")
```

Then, in accordance with the referenced table, use the following template to define profiles for each command:

RDEF OPERCMDS <systemcommandprofile> UACC(NONE) OWNER(<syspautd>) AUDIT(ALL(READ))

PERMIT <systemcommandprofile> CLASS(OPERCMDS) ID(<groupname>) ACCESS(<accesslevel>)

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-7485

Group Title: ACP00291

Rule ID: SV-7923r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00291](#)

Rule Title: The system programmer will ensure that the CONSOLxx members are properly configured.

Vulnerability Discussion: MCS consoles can be used to issue operator commands. Failure to properly control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(PARMLIB)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ACP00291)

Review each CONSOLxx parmlib member. If the following guidance is true, this is not a finding.

___ The "DEFAULT" statement for each CONSOLxx member specifies "LOGON(REQUIRED)" or "LOGON(AUTO)".

___ The "CONSOLE" statement for each console assigns a unique name using the "NAME" parameter.

___ The "CONSOLE" statement for each console specifies "AUTH(INFO)". Exceptions are the "AUTH" parameter is not valid for consoles defined with "UNIT(PRT)" and specifying "AUTH(MASTER)" is permissible for the system console.

Note: The site should be able to determine the system consoles. However, it is imperative that the site adhere to the "DEFAULT" statement requirement.

Fix Text: The Systems programmer should use the following recommendations and techniques to provide protection for MCS consoles:

Ensure that the DEFAULT statement specifies LOGON(REQUIRED) so that all operators are required to log on prior to entering z/OS system commands. At the discretion of the IAO, LOGON(AUTO) may be used.

Ensure that each CONSOLE statement specifies an explicit console NAME. And that AUTH(INFO) is specified, this also including extended MCS consoles. AUTH(MASTER) may be specified for systems console.

CCI: CCI-000382

CCI: CCI-002234

Group ID (Vulid): V-7486

Group Title: ACP00292

Rule ID: SV-7925r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00292](#)

Rule Title: MCS console userid(s) will be properly protected.

Vulnerability Discussion: MCS consoles can be used to issue operator commands. Failure to properly control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(PARMLIB)

Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- ACF2CMDS.RPT(LOGONIDS)
- ACF2CMDS.RPT(RULES)
- SENSITIVE.RPT(OPERCMDS)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Verify that the MCS console logonids are properly restricted. If the following guidance is true, this is not a finding.

_____ Each console defined in the currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) is associated with a valid ACF2 logonid.

_____ Each console logonid has no special privileges and/or attributes (e.g., ACCOUNT, SECURITY, etc.).

_____ Each console logonid has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.).

_____ Each console logonid will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMDS resource class and consolename in the CONSOLE resource class.

NOTE: If LOGON(AUTO) is specified in the currently active CONSOLxx parmlib member, additional access may be required. Permissions for the console logonids may be given with SERVICE(READ) to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resources.

NOTE: Execute the JCL in CNTL(ACFRPTRX) using the ACF2 console userids in the LID statements in the SYSIN input. This report lists all occurrences of these userids within the ACF2 database, including data set and resource access lists.

Fix Text: Memory and privileged program dump resources are provided via resources in the FACILITY resource class. Ensure that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Below is listed the access requirements for memory and privileged program dump resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent are followed. When protecting the facilities for dumps lists via the FACILITY resource class, ensure that the following items are in effect:

IEAABD.
IEAABD.DMPAUTH.
IEAABD.DMPAKEY.

The ACF2 resources are defined with a default access of PREVENT.

Ensure that no access is given to IEAABD. resource.

Example:

```
$KEY(IEAABD) TYPE(FAC)  
- UID(*) PREVENT
```

IEAABD.DMPAUTH. READ access is limited to authorized users that have a valid job duties requirement for access. UPDATE access will be restricted to system programming personnel and access will be logged.

Example:

```
$KEY(IEAABD) TYPE(FAC)  
DMPAUTH.- UID(syspautd) SERVICE(UPDATE) LOG  
DMPAUTH.- UID(authusers) SERVICE(READ)  
DMPAUTH.- UID(*) PREVENT
```

IEAABD.DMPAKEY. access will be restricted to system programming personnel and access will be logged.

Example:

```
$KEY(IEAABD) TYPE(FAC)  
DMPAKEY.- UID(syspautd) LOG  
DMPAKEY.- UID(*) PREVENT
```

CCI: CCI-000382

CCI: CCI-002232

Group ID (Vulid): V-7487
Group Title: ACP00293

Rule ID: SV-7928r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00293](#)

Rule Title: MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.

Vulnerability Discussion: MCS consoles can be used to issue operator commands. Failure to properly control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CONSOLE)

Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(CONSOLE)
- ACF2CMDS.RPT(RESOURCE) Alternate report

NOTE: If CLASMAP defines CONSOLE as anything other than the default of TYPE(CON), replace CON below with the appropriate three letters.

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00293)

Review resource rules for TYPE(CON). Ensure the following items are in effect for all MCS consoles identified in the EXAM.RPT(CONSOLE):

- 1) Each console is defined to ACF2 with a corresponding resource rule for TYPE(CON).
- 2) Each TYPE(CON) rule is defined with PREVENT access by default.
- 3) The logonid associated with each console has READ access to the corresponding resource defined in the CONSOLE resource class.
- 4) Access authorization for CONSOLE resources restricts READ access to operations and system programming personnel.

Fix Text: The IAO must ensure that all MCS consoles are defined to the CONSOLE resource class and READ access is limited to operators and system programmers.

Review the MCS console resources defined to z/OS and the ACP, and ensure they conform to those outlined below.

Each console defined in the CONSOLxx parmlib members is defined to ACF2 with a corresponding resource rule for TYPE(CON).

Each TYPE(CON) rule is defined with PREVENT access by default.

The logonid associated with each console has READ access to the corresponding resource defined in the CONSOLE resource class.

Access authorization for CONSOLE resources restricts READ access to operations and system programming personnel.

Example:

```
$KEY(MZNC20) TYPE(CON)
USERDATA(CONSOLE ID SECURITY)
UID(syspau) ALLOW
UID(operau) ALLOW
UID(MZNC20) ALLOW DATA(MZNC20 CONSOLE LOGONID ACCESS REQUIREMENTS)
UID(*) PREVENT
```

```
SET R(CON)
COMPILE 'ACF2.MZN.CON(MZNC20)' STORE
```

```
F ACF2,REBUILD(CON)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-7488

Group Title: ACP00294

Rule ID: SV-7931r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00294](#)

Rule Title: Users that have access to the CONSOLE resource in the TSOAUTH resource class are not properly defined.

Vulnerability Discussion: MCS consoles can be used to issue operator commands. Failure to properly control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(TSOAUTH)
- ACF2CMDS.RPT(ATTCONSL)
- ACF2CMDS.RPT(OPERPARM)
- SENSITIVE.RPT(OPERCMDS)
- ACF2CMDS.RPT(RESOURCE) Alternate report

NOTE: If CLASMAP defines TSOAUTH or OPERCMDS as anything other than the default of TYPE(TSO) or TYPE(OPR), replace TSO or OPR below with the appropriate three letters.

b) If the CONSOLE resource is not defined to the TSOAUTH resource class, there is NO FINDING.

c) At the discretion of the IAO, users may be allowed to issue z/OS system commands from a TSO session. With this in mind, ensure the following items are in effect for users granted the CONSOLE resource in the TSOAUTH resource class or users assigned the CONSOLE attribute:

- 1) Logonids are restricted to the INFO level on the AUTH field specified in the OPERPARM segment of the user profile record.
- 2) Logonids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the OPERCMDS resource class (i.e., resource rules for TYPE(OPR)).

d) If all of the above are true, there is NO FINDING.

e) If any of the above are untrue, this is a FINDING.

Fix Text: Evaluate the impact of correcting any deficiencies. Develop a plan of action and implement the required changes. Ensure the following items are in effect for all MCS consoles:

1. Define a profile protecting the use of the CONSOLE command within TSO. A sample command to accomplish this is shown here: RDEF TSOAUTH CONSOLE UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))

2. Permit only authorized users. A sample command to accomplish this is shown here: PE CONSOLE CL(TSOAUTH) ID(<syspautd>)
3. Set up the OPERPARM segment in corresponding user-class entry. A sample command to accomplish this is shown here: ALU <authorizeduser> OPERPARM(AUTH(INFO))
4. Userids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the OPERCMDS resource class. A sample command to accomplish this is shown here using the GLOBAL class:

RDEF GLOBAL OPERCMDS ADDMEM(MVS.MCSOPER.&RACUID/READ) OWNER(ADMIN)

CCI: CCI-000213

Group ID (Vulid): V-7558

Group Title: ACP00310

Rule ID: SV-8036r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00310](#)

Rule Title: Userids found inactive for more than 35 days are not suspended.

Vulnerability Discussion: Userid maintenance is critical in a C2 level of trust environment. Userids left on the system for extended periods of time could be reassigned to a different user while retaining the access authorizations of the previous user. The improper management of userids could result in the compromise of the operating system environment, ACP, and customer data.

Note: This vulnerability applies to inter

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, IAAC-1

Check Content:

Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(UNUSD35A)
- ACF2CMDS.RPT(UNUSD35C)
- ACF2CMDS.RPT(UNUSD35S)

Ensure that every interactive user shows an ACC-DATE=mm/dd/yy within the past 35 days.

NOTE: Valid for interactive USERIDS, not valid for Started task USERIDS and Batch USERIDS.

Fix Text:

The IAO must develop a procedure to check all userids for inactivity more than 35 days. If found, the IAO must suspend an account, but not delete it until it is verified by the local IAO that the user no longer requires access. If verification is not received within 60 days, the account may be deleted.

CCI: CCI-000017

Group ID (Vulid): V-3331

Group Title: ACP00320

Rule ID: SV-3331r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00320](#)

Rule Title: The ACP audit logs must be reviewed on a regular basis .

Vulnerability Discussion: Each ACP has the ability to produce audit records, based on specific security-related events. Audit Trail, Monitoring, Analysis and Reporting provides automated, continuous on-line monitoring and audit trail creation capability, to alert personnel of any unusual or inappropriate activity with potential IA implications. Failure to perform audit log analysis would allow for unusual or inappropriate activity to continue without review and appropriate actions taken.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

I. Audit Log - Daily Review

At a Minimum Weekly Review for the z/OS Level:

If the installation has the Vanguard Advisor product, run the Violation Detail report by selecting option 1 on the Advisor Main menu and then option 10, Violations Detail Report for Access Violations.

For invalid password attempts run Option 1 Standard Reports and then, Option 3 System Entry Summary Report. Hit enter for online report with No Masking specified. Look at the counts under the column Vios for the number of invalid logon attempts. Place an S next to any userid with Vios and review.

Look specifically for the following:

- 1) A User attempting to read/update/delete/scratch/alter a critical dataset which the STIG prohibits:
 - a) Security database files, and security setup (parmlib)
 - b) System parmlib such as SYS1.PARMLIB
- 2) A user generating violation(s) while attempting to update (or greater level) operating system datasets which they do not have access to:
 - a) SYS1*, SYS2*, SYS3*, SYS4*, SYS*
- 3) A user generating violation(s) while attempting to update (or greater level) APF libraries.
- 4) A user generating violation(s) while attempting Volume Level access.
- 5) Violations of JESSPOOL resources against domain level operations batch processing, system programmer submitted jobs, security related batch jobs and system level started tasks.
- 6) Violations generated against critical system level resources FACILITY/IBMFAC and OPERCMDS.
- 7) A review of users who incurred more than 10 password violations within a given day during the prior week as an indicator for further review and research of possible unusual activity.
- 8) The site may choose to monitor, at the discretion of the site, any additional critical system level resources they deem necessary above and beyond the above specified.

a) If any of the above unusual or inappropriate activity is found within the Audit Log records and documentation (email strings or other written documentation) exists showing actions were taken based upon the discovery of an unusual or inappropriate activity event, there is NO FINDING.

b) If any of the above unusual or inappropriate activity is found within the Audit Log records and NO documentation exists, this is a FINDING.

Fix Text: The site must provide a Security Log Management policy that documents and implements a process to review and analyze information system audit records every seven days or more frequently if required by the site Security Log Management policy. This process must contain an audit trail of reviews. Recommend NIST Special Publication 800-92, Guide to Computer Security Log Management as a guideline for establishing Log Management policy.

DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects,

security levels, or categories of information (e.g., classification levels), successful and unsuccessful logon attempts, privileged activities or other system level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module loads, unloads, and restarts.

Possible areas for review may be as follows:

- 1) A User attempting to read/update/delete/alter a critical dataset which the STIG prohibits:
 - a) Security database files, and security setup
 - b) System parmlib such as SYS1.PARMLIB
- 2) A user attempting to update (or greater access levels) system datasets which they would not have access to:
- c) SYS1*, SYS2*, SYS3*, SYS4*, etc.
- 3) A user generating violation(s) attempting to update (or greater access levels) APF libraries
- 4) A user generating violation(s) attempting Volume Level access
- 5) Violations of JESSPOOL resources against domain level operations batch processing, system programmer submitted jobs, security related batch jobs, and system level started tasks
- 6) Violations generated against critical system level resources FACILITY/IBMFAC and OPERCMDS
- 7) A weekly review of users' password violations within a given day during the prior week - is an indicator for further review and research of possible unusual activity
- 8) The site may choose to monitor, at the discretion of the site, any additional critical system level resources they deem necessary above and beyond the above specified

CCI: CCI-000148

Group ID (Vulid): V-3716

Group Title: ACP00330

Rule ID: SV-3716r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00330](#)

Rule Title: User accounts defined to the ACP do not uniquely identify system users.

Vulnerability Discussion: System users must be uniquely identified to the operating system. To accomplish this, each user must have an individual account defined to the ACP. If user accounts are not associated with specific individuals and are shared among multiple users, individual accountability is lost. This could hamper security audit activities and lead to unauthorized user access of system resources and customer data.

. Scope of, ownership of and responsibility over users shall be based upon the specifics of appointment, role, responsibilities and level of authority. Such as a domain/system level IAO is responsible for the Domain/system level users, whereas normally a application user would be the responsibility of the DoD AIS application security team unless SLA indicates otherwise.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

The IAO will provide a list of all userids that are shared among multiple users(i.e not uniquely identified system users).

b) If there are no shared userids on this domain, there is NO FINDING.

c) If there are shared userids on this domain, this is a FINDING.

NOTE: Userids should be able to be traced back to a current DD2875 or a Vendor Requirement (example: A Started Task).

Fix Text: The IAO wil identify user accounts defined to the ACP that are being shared among multiple users. This may require interviews with appropriate system-level support personnel. Remove the shared user accounts from the ACP.

The IAO is required to uniquely identify each system user to the ACP, and that access to resources is limited to those needed to perform the function. A user is defined as either an individual accessing a computer resource, or as a task executing on the system that requires access to a resource. On z/OS systems a user is identified by means of a unique userid. Security requires that audit data record the identity of the user, time of access, interaction with the system, and sensitive functions that might permit a user or program to modify, bypass, or negate security safeguards.

Any userid (user) on the system must be associated with only one individual also any given individual may be assigned responsibility for multiple userids on a given system, depending on functional responsibilities, to ensure task segregation.

CCI: CCI-000764

Group ID (Vulid): V-23837

Group Title: ACP00340

Rule ID: SV-28773r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00340](#)

Rule Title: z/OS Baseline reports are not reviewed and validated to ensure only authorized changes have been made within the z/OS operating system. This is a current DISA requirement for change management to system libraries.

Vulnerability Discussion: A product that generates reports validating changes, additions or removal from APF and LPA libraries, as well as changes to SYS1.PARMLIB PDS members, should be run against system libraries to provide a baseline analysis to allow monitoring of changes to these libraries. Failure to monitor and review these reports on a regular bases and validating any changes could threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCPR-1, DCSL-1, ECAT-1, ECAT-2

Check Content:

a) The z/OS Baseline reports (as indentified by report/function CS221C and CS243C) shall be reviewed and validated with the appropriate system programming staff on the period of time required by the current INFOCON level.

The first time you run this analysis, follow these steps to create a baseline:

1. Gather information on APF libraries: From the Analyzer Main Menu, choose Option 4 Batch reports and then I Link Pack Area Analysis. Put an S next to Authorized Program Facility (APF) Table. Make sure AC(1) module List is set to YES and all other OPTIONS are NO. Hit Enter, choose S to submit the JCL.
2. Gather information on LPA libraries: From the Analyzer Main Menu, choose Option 4 Batch reports and then OPTION B Sensitive/Critical Data Sets Analysis. Put an S next to Authorized Program Facility (APF) Table. Make sure all other OPTIONS are NO. Hit Enter, choose S to submit the JCL.
3. Now, create a copy of these reports for future reference. Find the jobs on the spool, put a ? next to the job and then XDC next to the DDNAME REPORT. Fill in the information for the output dataset naming the APF library Report with the last qualifier of CS221C and the LPA report with the last qualifier of CS243C.

The second and subsequent times you run this analysis (step 1 and 2 above) and compare the new reports with the previously generated reports.

Look for the following and validate that any changes are valid. If changes were made that are valid, repeat steps 1-3 above to create a new baseline.

APF library stats (# of libraries in APF list, # duplicate libraries in APF list, # accessible of libraries in APF list, # of members in APF libraries, # of members linked with AC=1, # of APF libraries in LINKLIST/LPA, # duplicate of APF libraries in LINKLIST/APF, # of accessible APF libraries in LINKLIST/LPA, #

of members in authorized LINKLIST/LPA, # of members links AC=1 in LINKLIST/LPA, total # of APF libraries, total # of unique APF libraries , total # of members with AC=1, total % of members with AC=1, APF datasets. This functional name will correspond to the dataset report file name that ends in CS221C .

LPA library display (LPA libraries added/removed, last accessed date for LPA libraries). This functional name will correspond to the dataset report file name that ends in CS243C .

Reports shall be compared with known and authorized changes to the specific z/OS domain. Any anomalies found shall be documented as a potential incident and must be investigated with written documentation as proof showing such review was completed.

b) If the baseline reports are being reviewed and samples of the reports exist, there is NO FINDING.

c) If the baseline reports are not being reviewed or samples of the reports do not exist this is a FINDING.

Fix Text: Validate the results of the z/OS Baseline reports with the appropriate system programming staff.

For sites that have CA-Auditor, minimally the following functional reports shall be validated: CS212C, CS221C and CS243C..

Compliance of this would be for the appropriate system programming staff to review the specific baseline reports and to affirm the changes are legitimate. Any identified exception or anomaly shall be reported, researched and documented. Such documentation shall be made available for auditor reviews.

The baseline reports should be created as GDGs, and should be saved for at least a year. Please see the z/OS Addendum under ACP00340 for additional instructions, and a sample of the CA-Auditor reports that should be run for that utilizes CA-Auditor.

CCI: CCI-000294

CCI: CCI-000295

CCI: CCI-000296

CCI: CCI-001819

CCI: CCI-001823

CCI: CCI-002087

Group ID (Vulid): V-29532

Group Title: ACP00350

Rule ID: SV-38886r5_rule

Severity: CAT II

Rule Version (STIG-ID): [ACP00350](#)

Rule Title: IEASYMUP resource will be protected in accordance with proper security requirements.

Vulnerability Discussion: Failure to properly control access to the IEASYMUP resource could result in unauthorized personnel modifying sensitive z/OS symbolics. This exposure may threaten the integrity and availability of the operating system environment.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Note: Generic profiles can be used (i.e. IEA*.* instead of IEASYMUP.*) for the checks below, as long as all the detailed requirements re access and logging as specified below, are met.

Ensure the following are in affect:

- a) A covering profile for IEASYMUP.* exists and is defined with UACC(NONE) and AUDIT is specified as SUCCESSES(UPDATE) and FAILURES(READ)
- b) Only systems programmers, DASD Administrators and Tape Librarians are in the access list with UPDATE access or higher
- c) To verify
 1. From the Administrator Main Menu Choose Option 3;4 (Security Server Reports, General Resource Profiles)
 2. Tab down to CLASS and enter FACILITY
 3. Tab down PROFILE and enter IEA*
 - 4) Find the covering profile for IEASYMUP.* and type LR next to it in the command line.

5) Review the output against the requirements in a. above...
d) If all of the above are TRUE, there is NO FINDING.
e) If either
- a covering profile is not found or
- audit logging per above (SUCSESSES (UPDATE), FAILURES(READ))
is not specified or
- personnel other than Systems Programmers, DASD Administrators or
Tape Librarians have UPDATE or higher access
then , there is a FINDING..

Fix Text: The IAO will ensure that the System level symbolic resources are defined to the FACILITY resource class and protected. UPDATE access to the System level symbolic resources are limited to System Programmers, DASD Administrators, and/or Tape Library personnel. All access is logged. Ensure the guidelines for the resources and/or generic equivalent are followed.

Limit access to the IEASYMUP resources to above personnel with UPDATE and/or greater access.

The following commands are provided as a sample for implementing resource controls:

```
rdef facility ieasymup.* uacc(none) owner(admin) -  
    audit(all(read)) -  
    data('protected per acp00350')  
rdef facility ieasymup.symbolname uacc(none) owner(admin) -  
    audit(all(read)) -  
    data('protected per acp00350')
```

```
pe ieasymup.symbolname cl(facility) id(<dasdaudt) acc(u)  
pe ieasymup.symbolname cl(facility) id(<syspaudt) acc(u)  
pe ieasymup.symbolname cl(facility) id(<tapeaudt) acc(u)
```

CCI: CCI-002234

Group ID (Vulid): V-69223

Group Title: ICERA010

Rule ID: SV-83837r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ICERA010](#)

Rule Title: All digital certificates in use must have a valid path to a trusted Certification authority.

Vulnerability Discussion: The origin of a certificate, the Certificate Authority (i.e., CA), is crucial in determining if the certificate should be trusted. An approved CA establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

Responsibility: N/A

IAControls: N/A

Check Content:

NOTE: The procedures in this checklist item presume the domain being reviewed is running all releases of z/OS, and use the ACP as the certificate store. If the domain being review is not a production system and is only used for test and development, this Self-Signed Certificates review can be skipped.

Refer to the following report produced by the ACF2 Data Collection Checklist:

ACF2CMDS.RPT(CERTRPT)

If no certificate information is found, there is NO FINDING.

NOTE: Certificates are only valid when their Status is TRUST. Therefore, you may ignore certificates with the NOTRUST status during the following checks.

If the digital certificate information indicates that the issuer's distinguished name leads to a DoD PKI Root Certificate Authority or External Certification Authority (ECA), there is no finding . Reference the IASE website for complete information as to which certificates are acceptable (<http://iase.disa.mil/pki-pke/interoperability/>).

Examples of an acceptable DoD CA are:

DoD PKI Class 3 Root CA

DoD PKI Med Root CA

Fix Text: Remove or and replace certificates whose the issuer's distinguished name does not lead to a DoD PKI Root Certification Authority, External Root Certification Authority (ECA), or an approved External Partner PKI s Root Certification Authority.

CCI: CCI-002470

Group ID (Vulid): V-69225

Group Title: ICERA020

Rule ID: SV-83841r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ICERA020](#)

Rule Title: Expired Digital Certificates must not be used.

Vulnerability Discussion: The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a relying Party that the unique binding between a key and its named subscriber is valid. Therefore, it is important that certificates are periodically refreshed. This is in accordance with DoD requirement. Expired Certificate must not be in use.

Responsibility: N/A

IAControls: N/A

Check Content:

NOTE: The procedures in this checklist item presume the domain being reviewed is running all releases of z/OS, and use the ACP as the certificate store.

The IAO will ensure that for production environments, expired certificates are not used.

If the domain being reviewed is not a production system and is only used for test and development, Expired Certificates review can be skipped.

a) From STIG ID ITCP0060, use the userid(s) assigned to the TCP/IP address space(s) and issue the following RACF command to list the certificate(s) associated with the TCPIP userid(s):

RACDCERT ID(tcpip userid) LIST

b) If no certificate information is found, there is NO FINDING.

NOTE: Certificates are only valid when their Status is TRUST. Therefore, you may ignore certificates with the NOTRUST status.

c) Check the expiration for each certificate with a status of TRUST. If the expiration date has passed this is a FINDING.

Fix Text: If the certificate is a user or device certificate with a status of TRUST, follow procedures to obtain a new certificate or re-key certificate. If it is an expired CA certificate remove it. _____

Group ID (Vulid): V-69227

Group Title: ICERA030

Rule ID: SV-83845r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ICERA030](#)

Rule Title: Certificate Name Filtering must be implemented with appropriate authorization and documentation.

Vulnerability Discussion: Certificate name filtering is a facility that allows multiple certificates to be mapped to a single ACP userid. Rather than matching a certificate stored in the ACP to determine the userid, criteria rules are used. Depending on the filter criteria, a large number of client certificates could be mapped to a single userid. Failure to properly control the use of certificate name filtering could result in the loss of individual identity and accountability.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

The IAO will ensure that certificate name filtering is not used unless the filtering rules have been documented to, and approved by, the IAM.

Currently the RACDCERT command does not support a generic userid value of ID(*) LISTMAP to list all the certificate name filters defined to RACF. However, the following commands can be issued to determine if certificate name filtering may be implemented.

- a) If certificate name filtering is in use, collect documentation describing each active filter rule and written approval from the ISSM to use the rule.
- b) Issue the SETROPTS LIST command. If the DIGTNMAP resource class is active, RACF is ready to process any certificate name filters with a Status of TRUST. The DIGTNMAP resource class should not be active unless certificate name filtering is desired.

If the DIGTNMAP resource class is not active, there is NO FINDING.

- c) Certificate name filters are stored as profiles in the DIGTNMAP resource class. The RLIST command is not intended for use with profiles in the DIGTNMAP resource class. However it can be used to determine if any profiles are defined. (NOTE: The information will not be displayed in a suitable format to easily interpret the filter.)

RLIST DIGTNMAP *

If there is nothing to list in the DIGTNMAP resource class, there is NO FINDING.

If profile information is displayed, one or more certificate name filters are defined to RACF. Under the NAME heading of each profile listing is the userid the filter is being mapped to. Issue the following command to list the certificate name filter associated with each userid:

Using Vanguard Administrators View Digital Mapping Filters option 18;2 with no masking review all Certificate name filters.

NOTE: Certificate name filters are only valid when their Status is TRUST. Therefore, you may ignore filters with the NOTRUST status.

- d) If the DIGTNMAP resource class is active and certificate name filters have a Status of TRUST, certificate name filtering is in use.

- e) If certificate name filtering is in use and filtering rules have been documented and approved by the ISSM, there is NO FINDING.
- f) If certificate name filtering is in use and filtering rules have not been documented and approved by the ISSM, this is a FINDING.

Fix Text: Ensure any certificate name filtering rules in use are documented and approved by the ISSM.

Group ID (Valid): V-3233

Group Title: IFTP0010

Rule ID: SV-13259r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0010](#)

Rule Title: The FTP Server daemon is not defined with proper security parameters.

Vulnerability Discussion: The FTP Server daemon requires special privileges and access to sensitive resources to provide its system services. Failure to properly define and control the FTP Server daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: N/A

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)
- ACF2CMDS.RPT(OMVSUSER)

Refer to the JCL procedure libraries defined to JES2.

b) Ensure the following items are in effect for the FTP daemon:

1) The FTP daemon is started from a JCL procedure library defined to JES2.

NOTE: The JCL member is typically named FTPD

2) The FTP daemon logonid is FTPD.

3) The FTPD logonid is defined with the STC attribute.

4) The FTPD logonid has the following z/OS UNIX attributes: UID(0), HOME directory / , shell program /bin/sh.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Evaluate the impact of correcting any deficiencies. Develop a plan of action and implement the required changes. Ensure the following items are in effect for all MCS consoles:

1. The FTP daemon userid must be FTPD and a matching entry in the STARTED resource class exists enabling the use of the standard userid and an appropriate group.
2. The FTPD userid is defined as a PROTECTED userid.
- 3) The FTPD userid has the following z/OS UNIX attributes: UID(0), HOME directory / , shell program /bin/sh.

Sample commands to accomplish these requirements are shown here:

Add the FTPD userid:

```
AU FTPD NAME('STC, FTP Daemon') NOPASSWORD NOOIDCARD DFLTGRP(STCTCPX) OWNER(STCTCPX) OMVS(UID(0) HOME('/')  
PROGRAM('/bin/sh'))
```

```
RDEF STARTED FTPD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) STDATA(USER(=MEMBER) GROUP(STCTCPX) TRACE(YES))
```

Additional permissions may be required. See SYS1.TCPIP.SEZAINST(EZARACF) or IBM Comm Server: IP Config Guide.

CCI: CCI-000764

Group ID (Vulid): V-3234

Group Title: IFTP0020

Rule ID: SV-3234r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0020](#)

Rule Title: The startup parameters for the FTP include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords. The FTP daemon s started task JCL does not specify the SYSTCPD and SYSFTPD DD statements for configuration files.

Vulnerability Discussion: During initialization, the FTP daemon reads JCL keywords and configuration files to determine values for critical operational parameters. Because system security is impacted by some of these parameter settings, controlling these options through the configuration file only and explicitly specifying the file locations reduces ambiguity, enhances security auditing, and ensures proper operations. Inappropriate values could result in undesirable

operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the startup parameters for the FTP daemon does not include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member. NOTE: The JCL member is typically named FTPD.

Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCP/IP started tasks.

b) Review the FTP daemon s started task JCL:

1. The SYSTCPD and SYSFTPD DD statements specify the TCP/IP Data and FTP Data configuration files respectively. _____ True _____ False

2. The ANONYMOUS keyword is not coded on the PARM parameter on the EXEC statement. _____ True _____ False

3. The ANONYMOUS=logonid combination is not coded on the PARM parameter on the EXEC statement. _____ True _____ False

4. The INACTIVE keyword is not coded on the PARM parameter on the EXEC statement. _____ True _____ FALSE

The AUTOLOG statement block can be configured to have TCP/IP start the FTP Server. The FTP entry (e.g., FTPD) can include the PARMSTRING parameter to pass parameters to the FTP procedure when started. NOTE: Parameters passed on the PARMSTRING parameter override parameters specified in the FTP procedure

c) Review the AUTOLOG statement block with in the PROFILE DD of the each

TCPIP started task JCL. If an FTP entry is configured in the AUTOLOG statement block in the TCP/IP Profile configuration file, ensure the following items are in effect:

1. The ANONYMOUS keyword is not coded on the PARMSTRING parameter.
2. The ANONYMOUS=logonid combination is not coded on the PARMSTRING parameter.
3. The INACTIVE keyword is not coded on PARMSTRING parameter.

d) If any items above are False this is a FINDING for STIG ID IFTPP020

Fix Text: Review the FTP daemon s started task JCL. Ensure that the ANONYMOUS and INACTIVE startup parameters are not specified and configuration file names are specified on the appropriate DD statements.

The FTP daemon program can accept parameters in the JCL procedure that is used to start the daemon. The ANONYMOUS and ANONYMOUS= keywords are designed to allow anonymous FTP connections. The INACTIVE keyword is designed to set the timeout value for inactive connections. Control of these options is recommended through the configuration file statements rather than the startup parameters.

The systems programmer responsible for supporting ICS will ensure that the startup parameters for the FTP daemon does not include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords.

During initialization the FTP daemon searches multiple locations for the TCPIP.DATA and FTP.DATA files according to fixed sequences. In the daemon s started task JCL, Data Definition (DD) statements will be used to specify the locations of the files. The SYSTCPD DD statement identifies the TCPIP.DATA file and the SYSFTPD DD statement identifies the FTP.DATA file.

The systems programmer responsible for supporting ICS will ensure that the FTP daemon s started task JCL specifies the SYSTCPD and SYSFTPD DD statements for configuration files.

Group ID (Vulid): V-3235

Group Title: IFTP0030

Rule ID: SV-3235r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0030](#)

Rule Title: FTP.DATA configuration statements for the FTP Server are not specified in accordance with requirements.

Vulnerability Discussion: The statements in the FTP.DATA configuration file specify the parameters and values that control the operation of the FTP Server components including the use of anonymous FTP. Several of the parameters must have specific settings to provide a secure configuration. Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the FTP Server FTP.DATA configuration statements are coded according to the settings in the OS390 STIG Volume 1 Table 4.4.41.3.a

FTP.DATA CONFIGURATION STATEMENTS

ANONYMOUS_ [Not Coded]

BANNER [An HFS file, e.g., /etc/ftp.banner]

INACTIVE_ [A value between 1 and 900]

UMASK_ 077

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member. NOTE: the JCL member is typically named FTPD.

b) Locate the SYSFTPD statement in all active FTPD started tasks JCL members executing on the domain.

c) From the ISPF Primary Option Menu use option 3.4 and review the FTP daemon s started task configuration identified by the SYSFTPD statement. Ensure the following items are in effect for the configuration statements specified in the FTP

Data configuration file:

1) The ANONYMOUS statement is not coded (does not exist) or, if it does exist, it is commented out. _____ True _____ False

NOTE: Other statements prefixed with ANONYMOUS may be present. These statements indicate the level of anonymous support and applicable restrictions if anonymous support is enabled using the ANONYMOUS statement. These other ANONYMOUS-prefixed statements may be ignored.

2) The INACTIVE statement is coded with a value between 1 and 900 (seconds). _____ True _____ False

NOTES: 900 indicates a session timeout value of 15 minutes.
0 disables the inactivity timer check.

3) The UMASK statement is coded with a value of 077. _____ True ____ False

4) The BANNER statement is coded. _____ True _____ FALSE

d) If any items above are False this is a FINDING for STIG ID IPFTP030

Fix Text: Review the configuration statements in the FTP.DATA file and ensure they conform to the specifications in the

FTP.DATA CONFIGURATION STATEMENTS below:

STATEMENT NOT CODED,
 CODED WITHOUT VALUE,
 OR PARAMETER VALUE

ANONYMOUS [Not Coded]

BANNER [An HFS file, e.g., /etc/ftp.banner]

INACTIVE [A value between 1 and 900]

UMASK 077 [See Note 1]

NOTE: If the FTP Server requires a UMASK value less restrictive than 077, requirements should be justified and documented with the IAO.

CCI: CCI-000048

CCI: CCI-000366

CCI: CCI-001133

Group ID (Vulid): V-3236

Group Title: IFTP0040

Rule ID: SV-3236r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0040](#)

Rule Title: User exits for the FTP Server are in use without proper approval or proper documentation.

Vulnerability Discussion: Several user exit points in the FTP Server component are available to permit customization of its operating behavior. These exits can be used to modify functions such as FTP command usage, client connection controls, post processing tasks, and SMF record modifications. Without proper review and adequate documentation of these exit programs, undesirable operations and degraded security may result. This exposure could lead to unauthorized access impacting data integrity or the availability of some system services, or contribute to the loss of accountability and hamper security audit activities.

Responsibility: Information Assurance Manager

IAControls: DCCS-1, DCCS-2, DCSL-1, DCSW-1

Check Content:

The systems programmer responsible for supporting ICS will ensure that the FTP Server user exits are not implemented.

- a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL. From the ISPF Primary Option Menu use option 3.4 and review the file(s) allocated by the STEPLIB DD statement in the FTP started task JCL.
 - 1. Refer to the libraries specified in the system Linklist and LPA.
 - 2. Refer to U_zOS_STIG_INSTRUCTION.doc for the information gathered from the IBM Communications Server Worksheet in the Preliminary Information Worksheets.
- b) Ensure the following items are in effect for FTP Server user exits:

The FTCHKCMD, FTCHKIP, FTCHKJES, FTCHKPWD, FTPSMFEX and FTPOSTPR modules are not located in the FTP daemon s STEPLIB, Linklist, or LPA.

NOTE: The ISPF ISRFIND utility can be used to search the system Linklist and LPA for specific modules.

Ensure that SMFEXIT= is not specified in the FTP DATA configuration file enabling the FTPSMFEX exit.

c) If both of the above are true, there is NO FINDING.

d) If any FTP Server user exits are implemented and the site has written approval from DISA FSO to install and use the exits, there is NO FINDING.

e) If any FTP Server user exits are implemented and the site has not obtained written approval from FSO to install and use the exits, this is a FINDING.

Fix Text: Review the configuration statements in the FTP.DATA file. Review the FTP daemon STEPLIB, system Linklist, and Link Pack Area libraries. If FTP Server exits are enabled or present, and have not been approved by the site IAM and not securely written and implemented by the site systems programmer, they should not be installed. Verify that non of the following exits are installed unless they have met the requirements listed above:

FTCHKCMD
FTCHKIP
FTCHKJES
FTCHKPWD
FTPOSTPR
FTPSMFEX

CCI: CCI-000382

CCI: CCI-001764

CCI: CCI-001765

Group ID (Vulid): V-3237

Group Title: IFTP0050

Rule ID: SV-3237r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0050](#)

Rule Title: The warning banner for the FTP Server is not specified properly.

Vulnerability Discussion: A logon banner can be used to inform users about the environment during the initial logon. In the DISA environment, logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Documentable: YES

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:

The systems programmer responsible for supporting ICS will ensure that for systems at Z/OS Release 2.10 and above, the FTP.DATA BANNER parameter specifies an HFS file or Z/OS data set that contains the warning logon banner.

- a) From the ISPF Primary Option Menu use option 3.4 and review the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.
- b) Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes

including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

Fix Text: Review the file specified by the FTP.DATA BANNER parameter. Ensure the text in this file specifies a logon banner in accordance with DISA requirements.

Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or z/OS data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-3238

Group Title: IFTP0060

Rule ID: SV-3238r4_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0060](#)

Rule Title: SMF recording options for the FTP Server must be configured to write SMF records for all eligible events.

Vulnerability Discussion: The FTP Server can provide audit data in the form of SMF records. The SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECAT-1, ECAT-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the FTP Server FTP.DATA configuration statements are coded according to the settings in the following table

- a) From the ISPF Primary Option Menu use option 3.4 and review the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.
- b) Ensure the following items are in effect for the configuration statements specified in the FTP Data configuration file:
 - 1. The SMF statement is coded with a value of STD.
 - 2. The SMFJES and SMFSQL statements are coded without an additional value.
 - 3. The SMFAPPE, SMFDEL, SMFEXIT, SMFLOGN, SMFREN, SMFRETR, and SMFSTOR statements are not coded or commented out.
- c) If all of the above are true, there is NO FINDING.
- d) If any of the above is untrue, this is a FINDING.

Fix Text: The system programmer will review the configuration statements in the FTP.DATA data set and ensure the SMF options conform to the specifications in the FTP.DATA Configuration Statements below or that they are commented out.

| | |
|---------|------------------------------|
| SMF | TYPE119 |
| SMFJES | TYPE119 |
| SMFSQL | TYPE119 |
| SMFAPPE | [Not coded or commented out] |
| SMFDEL | [Not coded or commented out] |
| SMFEXIT | [Not coded or commented out] |
| SMFLOGN | [Not coded or commented out] |
| SMFREN | [Not coded or commented out] |
| SMFRETR | [Not coded or commented out] |
| SMFSTOR | [Not coded or commented out] |

The FTP Server can provide audit data in the form of SMF records. SMF record type 119, the TCP/IP Statistics record, can be written with the following subtypes:

70 Append
70 Delete and Multiple Delete
72 Invalid Logon Attempt
70 Rename
70 Get (Retrieve) and Multiple Get
70 Put (Store and Store Unique) and Multiple Put

SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. This data may provide valuable information for security audit activities. Type 119 records use a more standard format and provide more information.

CCI: CCI-000130

CCI: CCI-000366

Group ID (Vulid): V-3239

Group Title: IFTP0070

Rule ID: SV-3239r3_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0070](#)

Rule Title: The permission bits and user audit bits for HFS objects that are part of the FTP Server component will be properly configured.

Vulnerability Discussion: HFS directories and files of the FTP Server provide the configuration and executable properties of this product. Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFTP0050)

NOTE: Additional Analysis will be required for the above file.

b) Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the FTP Server. Ensure they conform to the specifications in the table below:

| FTP Server HFS Object Security Settings | | |
|---|-----------------|-----------------|
| File | Permission Bits | User Audit Bits |
| /usr/sbin/ftpd | 1740 | fff |
| /usr/sbin/ftpdns | 1755 | fff |

```
/usr/sbin/tftpd    0644    faf
/etc/ftp.data      0744    faf
/etc/ftp.banner    0744    faf
```

The /usr/sbin/ftpd and /usr/sbin/ftpdns objects are symbolic links to /usr/lpp/tcpip/sbin/ftpd and /usr/lpp/tcpip/sbin/ftpdns respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

The TFTP Server does not perform any user identification or authentication, allowing any client to connect to the TFTP Server. Due to this lack of security, the TFTP Server will not be used. The TFTP Client is not secured from use.

The /etc/ftp.data file may not be the configuration file the server uses. It is necessary to check the SYSFTPD DD statement in the FTP started task JCL to determine the actual file.

The /etc/ftp.banner file may not be the banner file the server uses. It is necessary to check the BANNER statement in the FTP Data configuration file to determine the actual file.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7   rwx          (least restrictive)
6   rw-
3   -wx
2   -w-
5   r-x
4   r--
1   --x
0   ---          (most restrictive)
```

The possible audit bits settings are as follows:

```
f   log for failed access attempts
a   log for failed and successful access
-   no auditing
```

Some of the files listed above (e.g., /etc/ftp.data) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all files that do exist should have the specified permission and audit bit settings.

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/ftpd
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpd
```

```
chmod 1755 /usr/lpp/tcpip/sbin/ftpdns
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpdns
chmod 0744 /etc/ftp.data
chaudit w=sf,rx+f /etc/ftp.data
chmod 0744 /etc/ftp.banner
chaudit w=sf,rx+f /etc/ftp.banner
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-3240

Group Title: IFTP0080

Rule ID: SV-3240r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0080](#)

Rule Title: MVS data sets for the FTP Server are not properly protected.

Vulnerability Discussion: MVS data sets of the FTP Server provide the configuration and operational characteristics of this product. Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of customer data and some system services.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

The IAO will ensure that if present, the data set containing the FTP.DATA configuration file allows read access to all authenticated users and all other access is restricted to systems programming personnel. The IAO will ensure that all write and allocate access to the data set containing the FTP.DATA configuration file is logged. The IAO will ensure that if present, the data set containing the FTP banner file allows read access to all

a) Locate the SYSFTPD statement in all active FTPD started tasks JCL members executing on the domain..

b) Using Vanguard Administrator Ensure the following data set controls are in effect for the FTP Server:

1. Using On-line Access and Authorization option 4 review the profile protecting

the dataset identified in (A) UPDATE and ALTER access to the data set containing the FTP Data configuration file is restricted to systems programming personnel.

Document the protecting profile(s)

NOTE: READ access to all authenticated users is permitted.

2. Using AUDIT FLAGS option 3;3;2 review all profiles identified in (1) to ensure UPDATE and ALTER access to the data set containing the FTP Data configuration file is logged.

3. From the ISPF Primary Option Menu use option 3.4 and review the banner statement located in the FTP configuration file. Using On-line Access and Authorization option 4 review the profile protecting the dataset identified to ensure UPDATE and ALTER access to the data set containing the FTP banner file is restricted to systems programming personnel.

4. From the ISPF Primary Option Menu use option 3.4 and review the banner statement located in the FTP configuration file. Using AUDIT FLAGS option 3;3;2 review all profiles identified in (1) READ access to the data set containing the FTP banner file is permitted to all authenticated users.

NOTES:

The MVS data sets mentioned above are not used in every configuration. Absence of a data set will not be considered a FINDING.

The data set containing the FTP Data configuration file is determined by checking the SYSFTPD DD statement in the FTP started task JCL.

The data set containing the FTP banner file is determined by checking the BANNER statement in the FTP Data configuration file.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Review the data set access authorizations defined to the ACP for the FTP.DATA and FTP.BANNER files. Ensure these data sets are protected as follows:

The data set containing the FTP.DATA configuration file allows read access to all authenticated users and all other access is restricted to systems programming

personnel.

All write and allocate access to the data set containing the FTP.DATA configuration file is logged.

The data set containing the FTP banner file allows read access to all authenticated users and all other access is restricted to systems programming personnel.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-3241

Group Title: IFTP0090

Rule ID: SV-6924r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0090](#)

Rule Title: The TFTP Server program is not properly protected.

Vulnerability Discussion: The Trivial File Transfer Protocol (TFTP) Server, known as tftpd, supports file transfer according to the industry standard Trivial File Transfer Protocol. The TFTP Server does not perform any user identification or authentication, allowing any client to connect to the TFTP Server. Due to this lack of security, the TFTP Server will not be used. Failure to restrict the use of the TFTP Server may result in unauthorized access to the host. This exposure may impact the integrity, availability, and privacy of application data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- ACF2CMDS.RPT(ACFGSO)
- SENSITIVE.RPT(PROGRAM)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(IFTP0090)

- b) Ensure the following program controls are in effect for the TFTP Server:
 - 1) Programs TFTPDP and EZATD are defined in the GSO PPGM record.
 - 2) Program resources TFTPDP and EZATD are defined in the PROGRAM resource class.
 - 3) No access to the program resources TFTPDP and EZATD is permitted.
- c) If all items in (b) are true, there is NO FINDING.
- d) If any item (b) is untrue, this is a FINDING.

Fix Text: The IAO will ensure that the resource controls for the TFTP Server programs TFTPDP and EZATD and ensure all access is restricted.

Evaluate the impact of implementing the following change. Develop a plan of action and implement the change as required.

- 1) Ensure that the resource controls for the TFTP Server programs TFTPDP and EZATD and ensure all access is restricted.

Examples:

```
SET CONTROL(GSO)
CHANGE PPGM PGM-MASK(TFTPDP EZATD) ADD
```

```
F ACF2,REFRESH(PPGM)
```

```
$KEY(TFTPDP) TYPE(PGM)
UID(*) PREVENT
```

```
SET R(PGM)
COMPILE 'ACF2.MVA.PGM(TFTPDP)' STORE
```

```
F ACF2,REBUILD(PGM)
```

```
$KEY(EZATD) TYPE(PGM)
UID(*) PREVENT
```

```
SET R(PGM)
COMPILE 'ACF2.MVA.PGM(EZATD)' STORE
```

```
F ACF2,REBUILD(PGM)
```

CCI: CCI-001764

CCI: CCI-002235

Group ID (Vulid): V-8271

Group Title: IFTP0100

Rule ID: SV-8757r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0100](#)

Rule Title: FTP / Telnet unencrypted transmissions require Acknowledgement of Risk Letter(AORL)

Vulnerability Discussion: In addition to the data transmission being in the clear, the user credentials are also passed in the clear, which violates the control IAIA-1. As mitigation for this vulnerability, special consideration must be given to account maintenance and the types of user privileges associated with these accounts. Interception of the above information could result in the compromise of the operating system environment, ACP, and customer data.

Potential Impacts:

Information being passed in the clear can violate System and Data integrity.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, EBRU-1, ECCT-1, ECCT-2

Check Content:

The IAO will ensure that For batch jobs, the INPUT DD statement does not refer to in-stream data (i.e., "DD *") if that data contains a password.

a) Refer to U_zOS_STIG_INSTRUCTION.doc for the following items gathered from the File Transfer Protocol (FTP) Worksheet in the Preliminary Information Worksheets:

1. Item 5 (List of all FTP userids defined to the ACP database, including the function and purpose of each FTP userid.)

b) Ensure that an Acknowledgement of Risk Letter exist for all userids utilizing unencrypted communications.

c) If (b) is true, there is NO FINDING.

d) If (b) is untrue, this is a FINDING.

Fix Text: Ensure that an Acknowledgement of Risk Letter exist for all userids utilizing unencrypted communications.

CCI: CCI-000041

CCI: CCI-000042

CCI: CCI-001037

CCI: CCI-001499

Group ID (Vulid): V-29952

Group Title: IFTP0110

Rule ID: SV-39518r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IFTP0110](#)

Rule Title: FTP Control cards will be properly stored in a secure PDS file.

Vulnerability Discussion: FTP control cards carry unencrypted information such as userids, passwords and remote IP Addresses. Without a requirement to store this information separate from the JCL and in-stream JCL, it allows a security exposure by allowing read exposure to this information from anyone having access to the JCL libraries.

Responsibility: Information Assurance Officer

IAControls: IAIA-1, IAIA-2

Check Content:

a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFTP0050)

NOTE: Additional Analysis will be required for the above file.

b) Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

Fix Text: Create a list or spreadsheet of the locations where FTP control cards are stored, who should have access to those libraries and which applications the FTP control cards are for.

Add Columns for all people permitted access to the secured PDS.

Make sure that the FTP control Cards for each FTP are stored in a secure PDS and that they are not placed in the JCL libraries or in the in-stream JCL for each

FTP.

CCI: CCI-000202

Group ID (Vulid): V-3242

Group Title: ISLG0010

Rule ID: SV-3242r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ISLG0010](#)

Rule Title: The Syslog daemon is not started at z/OS initialization.

Vulnerability Discussion: The Syslog daemon, known as SYSLOGD, is a z/OS UNIX daemon that provides a central processing point for log messages issued by other z/OS UNIX processes. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. It is important that SYSLOGD be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that Syslogd is started at Z/OS system initialization.

NOTE: Syslogd may be started from the shell, a cataloged procedure (STC), or the BPXBATCH program. Additionally, other mechanisms (e.g., CONTROL-O) may be used to automatically start the Syslog daemon. To thoroughly analyze this PDI you may need to view the OS SYSLOG using SDSF, find the last IPL, and look for the initialization of Syslogd.

a) If the Syslog daemon Syslogd is started automatically during the initialization of the z/OS system, there is NO FINDING.

b) If (a) is untrue, this is a FINDING.

Fix Text: Review the files used to initialize tasks during system IPL (e.g., /etc/rc, SYS1.PARMLIB, CONTROL-O definitions) to ensure the Syslog daemon is automatically started during z/OS system initialization.

It is important that syslogd be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. As with other z/OS UNIX daemons, there is more than one way to start SYSLOGD. It can be started as a process in the /etc/rc file or as a z/OS started task.

CCI: CCI-000764

CCI: CCI-002234

Group ID (Vulid): V-3243

Group Title: ISLG0020

Rule ID: SV-7079r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ISLG0020](#)

Rule Title: The Syslog daemon must be properly defined and secured.

Vulnerability Discussion: The Syslog daemon, known as syslogd, is a zOS UNIX daemon that provides a central processing point for log messages issued by other zOS UNIX processes. It is also possible to receive log messages from other network-connected hosts. Some of the IBM Communications Server components that may send messages to syslog are the FTP, TFTP, zOS UNIX Telnet, DNS, and DHCP servers. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. Primarily because of the potential to use this information in an audit process, there is a security interest in protecting the syslogd process and its associated data.

The Syslog daemon requires special privileges and access to sensitive resources to provide its system services. Failure to properly define and control the Syslog daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: N/A

Check Content:

The systems programmer responsible for supporting ICS will ensure that Syslogd runs under its own user account. Specifically, it does not share the account defined for the Z/OS UNIX kernel.

The systems programmer responsible for supporting ICS will ensure that Syslogd runs with a job/started task name such as SYSLOGD that uniquely identifies it.

- 1) If you start SYSLOGD from MVS then ensure the following:
 - a) The SYSLOG daemon userid is SYSLOGD.
 - b) The SYSLOGD userid is defined as a PROTECTED userid.
 - c) The SYSLOGD userid has the following z/OS OMVS attributes: UID(0) HOME(/) PROGRAM(/bin/sh)
 - d) A matching entry in the STARTED class exists mapping the SYSLOGD started proc to the SYSLOGD userid.

To do the above:

Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the SYSLOGD started task. Document the USERID.

Using Vanguard Administrator User Detail by LID Masking Criteria = syslogd userid. Use the L command and review the USERID and ensure all items are in effect for the Syslog daemon:

- 2) If you start SYSLOGD from /etc/rc then ensure the following:
 - a) The _BPX_JOBNAME environment variable is set to assign a job name of SYSLOGD.

To do the above:

You will need to locate the /etc/rc file and locate the BPX_JOBNAME in it.

- c) If SYSLOGD is started from MVS then if b(1) is true, there is NO FINDING.
- d) If SYSLOGD is started from within USS then if b(2) is true, there is NO FINDING.
- e) If SYSLOGD is started from within MVS and b(1) is untrue, this is a FINDING.
- f) If SYSLOGD is started from within USS and b(2) is untrue, this is a FINDING.

Fix Text: The IAO working with the systems programmer responsible for supporting IBM Comm Server will ensure that Syslog daemon runs under its own user account. Specifically, it does not share the account defined for the z/OS UNIX kernel.

The Syslog daemon userid is SYSLOGD.

The SYSLOGD userid is defined as a PROTECTED userid.

The SYSLOGD userid has UID(0), HOME(/), and PROGRAM(/bin/sh) specified in the OMVS segment.

To set up and use as an MVS Started Proc, the following sample commands are provided:

```
AU SYSLOGD NAME('stc, tcpip') NOPASSWORD NOOIDCARD DFLTGRP(STC)
OWNER(STC) DATA('Reference ISLG0020 for proper setup ')
ALU SYSLOGD DFLTGRP(stctcpx)
ALU SYSLOGD OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))
CO SYSLOGD GROUP(stctcpx) OWNER(stctcpx)
```

A matching entry mapping the SYSLOGD started proc to the SYSLOGD userid is in the STARTED resource class.

```
RDEF STARTED SYSLOGD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) STDATA(USER(SYSLOGD) GROUP(STC))
```

If /etc/rc is used to start the Syslog daemon ensure that the _BPX_JOBNAME and _BPX_USERID environment variables are assigned a value of SYSLOGD.

CCI: CCI-000764

Group ID (Vulid): V-3244

Group Title: ISLG0030

Rule ID: SV-3244r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ISLG0030](#)

Rule Title: The permission bits and user audit bits for HFS objects that are part of the Syslog daemon component will be configured properly.

Vulnerability Discussion: HFS directories and files of the Syslog daemon provide the configuration and executable properties of this product. Failure to properly secure these objects could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the permission bits and user audit bits for HFS objects that are part of the Syslog daemon component are

configured according to the settings in the following table:

SYSLOG DAEMON HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE PERMISSION BITS USERAUDIT BITS

| | | |
|-------------------|------|-----|
| /usr/sbin/syslogd | 1740 | fff |
| /etc/syslog.conf | 0744 | faf |

[Output log file defined in the configuration file]

| | |
|------|-----|
| 0744 | fff |
|------|-----|

a) Using Vanguard Administrator UNIX file manager option 14 review the files listed in the table above.

b) If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in this table, there is NO FINDING.

NOTES:

The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The /etc/syslog.conf file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file.

For example, in /etc/rc:

```
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf
```

For example, in the SYSLOGD started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT  
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'
```

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT  
// PARM='POSIX(ON) ALL31(ON) /-f /"SYS1.TCPPARMS(SYSLOG)'"
```

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx(least restrictive)
6 rw
3 -wx
2 w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
-no auditing

c) If any item in (b) is untrue, this is a FINDING.

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the Syslog daemon. Ensure they conform to the specifications in the SYSLOG Daemon HFS Object Security Settings table below.

Log files should have security that prevents anyone except the syslogd process and authorized maintenance jobs from writing to or deleting them.

A maintenance process to periodically clear the log files is essential. Logging stops if the target file system becomes full.

SYSLOG Daemon HFS Object Security Settings

| File | Permission Bits | User Audit Bits |
|---|-----------------|-----------------|
| /usr/sbin/syslogd | 1740 | fff |
| [Configuration File] | | |
| /etc/syslog.conf | 0744 | faf |
| [Output log file defined in the configuration file] | | |
| | 0744 | fff |

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)

| | | |
|---|-----|--------------------|
| 6 | rw- | |
| 3 | -wx | |
| 2 | -w- | |
| 5 | r-x | |
| 4 | r-- | |
| 1 | --x | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

NOTES:

The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The /etc/syslog.conf file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file. For example, in /etc/rc:

```
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf
```

For example, in the SYSLOGD started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'
```

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f /"SYS1.TCPPARMS(SYSLOG)'"
```

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/syslogd
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd
chmod 0744 /etc/syslog.conf
chaudit w=sf,rx+f /etc/syslog.conf
chmod 0744 /log_dir/log_file
chaudit rwx=f /log_dir/log_file
```

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-3215

Group Title: ITCP0010

Rule ID: SV-3215r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0010](#)

Rule Title: Configuration files for the TCP/IP stack are not properly specified.

Vulnerability Discussion: The TCP/IP stack reads two configuration files to determine values for critical operational parameters. These file names are specified in multiple locations and, depending on the process, are referenced differently. Because system security is impacted by some of the parameter settings, specifying the file names explicitly in each location reduces ambiguity and ensures proper operations. Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the TCP/IP started task s JCL specifies the PROFILE and SYSTCPD DD statements for the PROFILE.TCPIP and TCPIP.DATA configuration files and TCP/IP started task s JCL includes the RESOLVER_CONFIG variable, set to the name of the file specified on the SYSTCPD DD statement.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. If TCPIP is inactive, review the procedure libraries defined to JES2 and locate the TCPIP JCL member.
- b) Use IBM s dslist utility and review the TCPIP JCL to ensure the following items are in effect for the TCPIP started task JCL:

1. The PROFILE and SYSTCPD DD statements specify the TCP/IP Profile and Data configuration files respectively.
 2. The RESOLVER_CONFIG variable on the EXEC statement is set to the same file name specified on the SYSTCPD DD statement.
- c) If both of the above are true, there is NO FINDING.
- d) If either of the above is untrue, this is a FINDING.

Fix Text: Review the TCP/IP started task JCL to ensure the configuration file names are specified on the appropriate DD statements and parameter option.

During initialization the TCP/IP stack uses fixed search sequences to locate the PROFILE.TCPIP and TCPIP.DATA files. However, uncertainty is reduced and security auditing is enhanced by explicitly specifying the locations of the files. In the TCP/IP started task s JCL, Data Definition (DD) statements can be used to specify the locations of the files. The PROFILE DD statement identifies the PROFILE.TCPIP file and the SYSTCPD DD statement identifies the TCPIP.DATA file.

The location of the TCPIP.DATA file can also be specified by coding the RESOLVER_CONFIG environment variable as a parameter of the ENVAR option in the TCP/IP started task s JCL. In fact, the value of this variable is checked before the SYSTCPD DD statement by some processes. However, not all processes (e.g., TN3270 Telnet Server) will access the variable to get the file location. Therefore specifying the file location explicitly, both on a DD statement and through the RESOLVER_CONFIG environment variable, reduces ambiguity.

The systems programmer responsible for supporting ICS will ensure that the TCP/IP started task s JCL specifies the PROFILE and SYSTCPD DD statements for the PROFILE.TCPIP and TCPIP.DATA configuration files and TCP/IP started task s JCL includes the RESOLVER_CONFIG variable, set to the name of the file specified on the SYSTCPD DD statement.

CCI: CCI-000366

Group ID (Vulid): V-3216

Group Title: ITCP0020

Rule ID: SV-3216r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0020](#)

Rule Title: TCPIP.DATA configuration statements for the TCP/IP stack will be properly specified.

Vulnerability Discussion: During the initialization of TCP/IP servers and clients, the TCPIP.DATA configuration file provides information that is essential for proper operations of TCP/IP applications. Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the TCPIPJOBNAME, HOSTNAME, DOMAINORIGIN, DATASETPREFIX, and NSINTERADDR statements are coded in the TCPIP.DATA file.

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP.DATA configuration file.

b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Data configuration file:

1. TCPIPJOBNAME
2. HOSTNAME
3. DOMAINORIGIN/DOMAIN (The DOMAIN statement is functionally equivalent to the DOMAINORIGIN Statement)
4. DATASETPREFIX

c) If both of the above are true, there is NO FINDING.

d) If either of the above is untrue, this is a FINDING.

Fix Text: The system programmer will review the configuration statements in the TCPIP.DATA file and ensure they conform to the specifications below:

TCPIPJOBNAME - Specifies the job name of the TCP/IP address space. This name is also used as part of the name of some network security resources.

HOSTNAME - Specifies the TCP/IP host portion of the DNS name of the system.

DOMAINORIGIN/DOMAIN - Specifies the default domain name used for DNS searches.

DATASETPREFIX - Specifies the high-level qualifier to be used to dynamically allocate other configuration data sets.

The TCPIP.DATA file acts as the anchor configuration data set for the TCP/IP stack and all TCP/IP servers and clients running in z/OS. During the initialization of TCP/IP servers and clients, the TCPIP.DATA file provides basic information that is essential for proper operation.

The above TCPIP.DATA configuration parameters provide crucial information to TCP/IP applications.

CCI: CCI-000366

Group ID (Vulid): V-5627

Group Title: ITCP0025

Rule ID: SV-5627r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0025](#)

Rule Title: The hosts identified by the NSINTERADDR statement will be properly protected.

Vulnerability Discussion: If the hosts identified by NSINTERADDR statement are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the host and the hosts' components. Therefore, they can interfere with the normal operations of the host. Improper control of hosts and the hosts' components could compromise network operations.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, PEPF-1

Check Content:

The IAO will ensure that if any NSINTERADDR statements are coded in the TCPIP.DATA file, they refer to hosts connected directly to networks within the physical premises of the host site and located in areas with physical access limited to authorized personnel.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Refer to the Data configuration file specified on the SYSTCPD DD statement in the TCPIP started task JCL.
- b) Use IBM s dslist utility and review the TCPIP configuration file. Ensure the following items are in effect for the NSINTERADDR statements specified in the TCP/IP Data configuration file:
 - 1. The NSINTERADDR statements refer to hosts connected directly to networks

within the physical premises of the host site.

2. The NSINTERADDR statements refer to hosts that are located in areas with physical access limited to authorized personnel.

c) If both of the above are true, there is NO FINDING.

d) If either of the above is untrue, this is a FINDING.

Fix Text: The IAO will ensure that the hosts and the hosts components identified in the NSINTERADDR statement are protected.

The IAO, with assistance from the system programmer, will ensure that any NSINTERADDR statements coded in the TCPIP.DATA file refer to hosts connected directly to networks within the physical premises of the host site and located in areas with physical access limited to authorized personnel.

CCI: CCI-000366

CCI: CCI-000919

Group ID (Vulid): V-3217

Group Title: ITCP0030

Rule ID: SV-3217r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0030](#)

Rule Title: PROFILE.TCPIP configuration statements for the TCP/IP stack are not coded properly.

Vulnerability Discussion: The PROFILE.TCPIP configuration file provides system operation and configuration parameters for the TCP/IP stack. Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the DELETE statement is not coded in PROFILE.TCPIP files for production systems.

The systems programmer responsible for supporting ICS will ensure that the SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.

The systems programmer responsible for supporting ICS will ensure that the SMFPARMS statement is not used.

The systems programmer responsible for supporting ICS will ensure that the TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP.DATA configuration file.

b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

1. The SMFPARMS statement is not coded or commented out.
2. The DELETE statement is not coded or commented out for production systems.
3. The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.
4. The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

Fix Text: Review the configuration statements in the PROFILE.TCPIP file and ensure they conform to the specifications below:

Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

- 1) The SMFPARMS statement is not coded or commented out.
- 2) The DELETE statement is not coded or commented out for production systems.
- 3) The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.
- 4) The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance in STIG ID ITCP0070.

BASE TCP/IP PROFILE.TCPIP CONFIGURATION STATEMENTS FUNCTIONS

INCLUDE- Specifies the name of an MVS data set that contains additional PROFILE.TCPIP statements to be used
- It Alters the configuration specified by previous statements

SMFPARMS- Specifies SMF logging options for some TCP applications; replaced by SMFCONFIG
- Controls collection of audit data

DELETE- Specifies some previous statements, including PORT and PORTRANGE, that are to be deleted
- Alters the configuration specified by previous statements

SMFCONFIG- - Specifies SMF logging options for Telnet, FTP, TCP, API, and stack activity
- Controls collection of audit data

TCPCONFIG- Specifies various settings for the TCP protocol layer of TCP/IP
- Controls port access

CCI: CCI-000366

Group ID (Vulid): V-3218

Group Title: ITCP0040

Rule ID: SV-3218r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0040](#)

Rule Title: The permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component must be configured properly.

Vulnerability Discussion: HFS directories and files of the Base TCP/IP component provide the configuration, operational, and executable properties of IBMs TCP/IP system product. Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Refer to the file(s) allocated by the STEPLIB DD statement in the FTP started task JCL.

Refer to the libraries specified in the system Linklist and LPA.

If any FTP Server exits are in use, identify them and validate that they were reviewed for integrity and approved by the site AO.

b) Ensure the following items are in effect for FTP Server user exits:

The FTCHKCMD, FTCHKIP, FTCHKJES, FTCHKPWD, FTPSMFEX and FTPOSTPR modules are not located in the FTP daemon s STEPLIB, Linklist, or LPA.

NOTE: The ISPF ISRFIND utility can be used to search the system Linklist and LPA for specific modules.

c) If both of the above are true, there is no finding.

d) If any FTP Server user exits are implemented and the site has written approval from site ISSM to install and use the exits, there is no finding.

e) If any FTP Server user exits are implemented and the site has not had the site systems programmer verify the exit was securely written and installed, this is a finding.

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the Base TCP/IP component. Ensure they conform to the specifications in the BASE TCP/IP HFS Object Security Settings below:

BASE TCP/IP HFS Object Security Settings

| File | Permission Bits | User Audit Bits |
|------------------|-----------------|-----------------|
| /etc/hosts | 0744 | faf |
| /etc/protocol | 0744 | faf |
| /etc/resolv.conf | 0744 | faf |
| /etc/services | 0740 | faf |

```
/usr/lpp/tcpip/sbin    0755    faf
/usr/lpp/tcpip/bin     0755    faf
```

Some of the files listed above (e.g., /etc/resolv.conf) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all directories and files that do exist will have the specified permission and audit bit settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7   rwx      (least restrictive)
6   rw-
3   -wx
2   -w-
5   r-x
4   r--
1   --x
0   ---      (most restrictive)
```

The possible audit bits settings are as follows:

```
f   log for failed access attempts
a   log for failed and successful access
-   no auditing
```

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 0744 /etc/hosts
chaudit w=sf,rx+f /etc/hosts
chmod 0744 /etc/protocol
chaudit w=sf,rx+f /etc/protocol
chmod 0744 /etc/resolv.conf
chaudit w=sf,rx+f /etc/resolv.conf
chmod 0740 /etc/services
chaudit w=sf,rx+f /etc/services
chmod 0755 /usr/lpp/tcpip/bin
chaudit w=sf,rx+f /usr/lpp/tcpip/bin
chmod 0755 /usr/lpp/tcpip/sbin
chaudit w=sf,rx+f /usr/lpp/tcpip/sbin
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-3219

Group Title: ITCP0050

Rule ID: SV-7083r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0050](#)

Rule Title: TCP/IP resources must be properly protected.

Vulnerability Discussion: The Communication Server access authorization is used to protect TCP/IP resources such as stack, network, port, and other SERVAUTH resources. These resources provide additional security checks for TCP/IP users. Failure to properly secure these TCP/IP resources could lead to unauthorized user access resulting in the compromise of some system services and possible compromise of data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFTP0050)

NOTE: Additional Analysis will be required for the above file.

b) Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

Fix Text: The IAO must develop a plan of action to implement the required changes. Ensure the following items are in effect for TCP/IP resources.

(Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource class, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Ensure that the EZA, EZB and IST resources and/or generic equivalent are defined to the SERVAUTH resource class with a UACC(NONE)

No access is given to the EZA, EZB, and IST resources of the SERVAUTH resource class.

If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the SERVAUTH resource class. EZB.CSSMTP.sysname.writename.JESnode will be specified and made available to the CSSMTP started task and authenticated users that require access to use CSSMTP for e-mail services.

Only authenticated users that require access are permitted access to the second level of the resources in the SERVAUTH resource class. Examples are the network (NETACCESS), port (PORTACCESS), stack (STACKACCESS), and FTP resources in the SERVAUTH resource class.

The EZB.STACKACCESS. resource access authorizations restrict access to those started tasks with valid requirements and users with valid FTP access requirements.

The EZB.FTP.*.*.ACCESS.HFS) resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement

exists to access OMVS files and Directories.

The following commands are provided as a sample for implementing resource controls:

```
RDEF SERVAUTH EZB.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.sysname.writename.JESnode UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.FTP.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.NETACCESS.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.PORTACCESS.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.STACKACCESS.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
```

```
PE EZB.CSSMTP.sysname.writename.JESnode CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.sysname.ftpstc.ACCESS.HFS CL(SERVAUTH) ID(ftpprofile) ACC(READ)
PE EZB.NETACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.PORTACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.sysname.TCPIP CL(SERVAUTH) ID(ftpprofile) ACC(READ)
```

The following notes apply to these controls:

- EZB.STACKACCESS.sysname.TCPIP access READ should be limited to only those started tasks that require access to the TCPIP Stack as well as any users approved for FTP Access (inbound and/or outbound). FTP users should not have access to the EZB.FTP.sysname.ftpstc.ACCESS.HFS resource unless specific written justification documenting valid requirement for those FTP users to access USS files and directories via FTP.
- To be effective in restricting access, the network (EZB.NETACCESS) resource control requires configuration of the NETACCESS statement in the PROFILE.TCPIP file.
- To be effective in restricting access, the port (EZB.PORTACCESS) resource control requires configuration of a PORT or PORTRANGE statement in the PROFILE.TCPIP file. These port definitions within PROFILE.TCPIP shall be defined to include SAF keyword and a valid name.

A list of possible SERVAUTH resources defined to the first two nodes is shown here: (Note that additional resources may be developed with each new release of TCPIP.)

```
EZA.DCAS.
EZB.BINDDVIPARANGE.
EZB.CIMPROV.
EZB.FRCAACCESS.
EZB.FTP.
```

EZB.INITSTACK.
EZB.IOCTL.
EZB.IPSECCMD.
EZB.MODDVIPA.
EZB.NETACCESS.
EZB.NETMGMT.
EZB.NETSTAT.
EZB.NSS.
EZB.NSSCERT.
EZB.OSM.
EZB.PAGENT.
EZB.PORTACCESS.
EZB.RPCBIND.
EZB.SOCKOPT.
EZB.SNMPAGENT.
EZB.STACKACCESS.
EZB.TN3270.
IST.NETMGMT.

CCI: CCI-000213

Group ID (Vulid): V-3220

Group Title: ITCP0060

Rule ID: SV-7087r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0060](#)

Rule Title: Started tasks for the Base TCP/IP component must be defined in accordance with security requirements.

Vulnerability Discussion: The TCP/IP started tasks require special privileges and access to sensitive resources to provide its system services. Failure to properly define and control these TCP/IP started tasks could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)
- ACF2CMDS.RPT(OMVSUSER)

If the following items are true for the logonid(s) assigned to the TCP/IP address space(s), this is not a finding.

- ___ Named TCPIP or, in the case of multiple instances, prefixed with TCPIP
- ___ Defined with the STC, MUSASS, and NO-SMC attributes
- ___ z/OS UNIX attributes: UID(0), HOME directory / , shell program /bin/sh

If the following items are in effect for the logonid assigned to the EZAZSSI started task, this is not a finding.

- ___ Named EZAZSSI
- ___ Defined with the STC attribute
- ___ z/OS UNIX attributes: UID(non-zero), HOME directory / , shell program /bin/sh

Fix Text: The ISSO will ensure that the Started tasks for the Base TCP/IP component user accounts are defined with the following characteristics:

- Named TCPIP or, in the case of multiple instances, prefixed with TCPIP
- Defined with the STC, MUSASS, and NO-SMC attributes
- z/OS UNIX attributes: UID(0), HOME directory / , shell program /bin/sh
- Named EZAZSSI
- Defined with the STC attribute
- z/OS UNIX attributes: UID(non-zero), HOME directory / , shell program /bin/sh

Review the TCP/IP started task accounts, privileges, and access authorizations defined to the ACP. Ensure they conform to the requirements as outlined below.

The following commands can be used to create the user accounts that are required for the TCP/IP address space and the EZAZSSI started task:

```
SET LID
INSERT TCPIP NAME(TCPIP) GROUP(STCTCPX) STC MUSASS NO-SMC
INSERT EZAZSSI NAME(EZAZSSI) GROUP(STCTCPX) STC
```

```
SET PROFILE(USER) DIVISION(OMVS)
INSERT TCPIP UID(0) HOME(/) OMVSPGM(/bin/sh)
INSERT EZAZSSI UID(non-zero) HOME(/) OMVSPGM(/bin/sh)
```

```
F ACF2,REBUILD(USR),CLASS(P)
```

NOTE: At eTrust CA-ACF2 6.4 and above, the PROGRAM field in the user profile record has been renamed to OMVSPGM.

The following additions to the indicated rule sets can be used to assign the privileges that are required for the TCP/IP address space:

\$KEY(BPX) TYPE(FAC)

DAEMON UID(TCPIP-uid) SERVICE(READ) ALLOW

If the z/OS host machine has hardware encryption installed and enabled, resources owned by the Integrated Cryptographic Service Facility (ICSF) component have been defined. The following rule set additions are required to allow the TN3270 Telnet Server process to access the ICSF resources.

- \$KEY(CSFCKI) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFCKM) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFDEC) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFENC) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFOWH) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFRNG) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFPKB) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFPKX) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFPKE) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFPKD) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFPKI) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFD SG) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- \$KEY(CSFDSV) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW

The following operator commands are required to complete the updates:

F ACF2,REBUILD(FAC)

F ACF2,REBUILD(CSF)

These commands and definitions assume that the default type code for CSFSERV resources is CSF.

CCI: CCI-000764

Group ID (Vulid): V-3221

Group Title: ITCP0070

Rule ID: SV-3221r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ITCP0070](#)

Rule Title: MVS data sets for the Base TCP/IP component are not properly protected,

Vulnerability Discussion: MVS data sets of the Base TCP/IP component provide the configuration, operational, and executable properties of IBMs TCP/IP system product. Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1

Check Content:

The IAO will ensure that update, create, and scratch access to product data sets are restricted to systems programming personnel.

The IAO will ensure that update, create, and scratch access to the data set(s) containing the TCPIP.DATA and PROFILE.TCPIP configuration files are restricted to systems programming personnel and are logged.

The IAO will ensure that update, create, and scratch access to the data set(s) containing the configuration files shared by TCP/IP applications are restricted to systems programming personnel.

The IAO will ensure that write and allocate access to the data set(s) specified in the INCLUDE statements are restricted to systems programming personnel and are logged.

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate and document the configuration file identified by the PROFILE DD statement. Locate

and document the Data File identified by the SYSTCPD DD statement.

NOTE: Record the covering dataset profile for use in later steps.

b) Ensure the following controls are in effect for the Base TCP/IP component:

1. Using Vanguard Administrator On-line Access and Authorization option

4. Supply the datasets documented above and ensure UPDATE and ALTER access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix SYS1.TCPIP.AEZA and target data sets with the prefix SYS1.TCPIP.SEZA).

2. Using Vanguard Administrator On-line Access and Authorization option

4. Supply the dataset names documented above. Review the access and ensure UPDATE and ALTER access to the data set(s) containing the Data and Profile configuration file is restricted to systems programming personnel.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

3. Using Vanguard Administrator Audit Flags Report option 3;3;2. Supply the datasets documented above. All UPDATE and ALTER access to the data set(s) containing the Data and Profile configuration files is logged.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same logging requirements.

4. Using Vanguard Administrator On-line Access and Authorization option

4. Supply the dataset name for the configuration file documented above. Review the access and ensure UPDATE and ALTER access to the data set(s) containing the configuration files shared by TCP/IP applications is restricted to systems programming personnel.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Review with the IAO the data set access authorizations defined to the ACP for the Base TCP/IP component. Ensure these data sets are protected in accordance with the following rules:

WRITE and ALLOCATE access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix SYS1.TCPIP.AEZA and target data sets with the prefix SYS1.TCPIP. SEZA).

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is restricted to systems programming personnel.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is logged.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same logging requirements.

WRITE and ALLOCATE access to the data set(s) containing the configuration files shared by TCP/IP applications is restricted to systems programming personnel.

NOTE: For systems running the TSS ACP replace the WRITE and ALLOCATE with WRITE, UPDATE, CREATE, CONTROL, SCRATCH, and ALL.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-3222

Group Title: ITNT0010

Rule ID: SV-3222r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ITNT0010](#)

Rule Title: PROFILE.TCPIP configuration statements for the TN3270 Telnet Server are not properly specified.

Vulnerability Discussion: The PROFILE.TCPIP configuration file provides system operation and configuration parameters for the TN3270 Telnet Server. Several of these parameters have potential impact to system security. Failure to code the appropriate values could result in unexpected operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that unless documented with the IAM, a TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900. Exceptions are documented with the IAO.

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP or TN3270 started task. Locate the configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the profile Data configuration file.

b) Ensure the following items are in effect for the configuration statements specified in the Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

TELNETGLOBAL Block (only one defined)

1. The KEYRING statement, if used, is only coded within the TELNETGLOBALS statement block.
2. The KEYRING statement, if used, specifies the SAF parameter.

TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992)

1. The TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900.

NOTE: Effective in z/OS release 1.2, the INACTIVE statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

1. The TELNETPARMS TKOSPECLURECON statement is not coded or commented out.

BEGINVTAM Block (one or more defined)

2. The BEGINVTAM RESTRICTAPPL statement is not be coded or commented out.

c) If all of the above are true, there is NO FINDING.

d) If any of the above is untrue, this is a FINDING.

Fix Text: Review the configuration statements in the PROFILE.TCPIP file and ensure they conform to the specifications below:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

The KEYRING statement, if used, is only coded within the TELNETGLOBALS statement block.

The KEYRING statement, if used, specifies the SAF parameter.

"TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992) "

The TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900.

INACTIVE statements should not be coded with a value greater than 900 or 0. 0 disables the inactivity timer check.

NOTE: Effective in z/OS release 1.2, the INACTIVE statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

The TELNETPARMS TKOSPECLURECON statement should not be coded or it should be commented out.

BEGINVTAM Block (one or more defined)

The BEGINVTAM RESTRICTAPPL statement is not be coded or it should be commented out.

Group ID (Vulid): V-3223

Group Title: ITNT0020

Rule ID: SV-3223r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ITNT0020](#)

Rule Title: VTAM session setup controls for the TN3270 Telnet Server are not properly specified.

Vulnerability Discussion: After a connection from a Telnet client to the TN3270 Telnet Server has been established, the process of session setup with a VTAM application occurs. A number of BEGINVTAM statements must be coded in a specific configuration to ensure adequate control to VTAM applications is maintained. Failure to code the appropriate statements could result in unauthorized access to the host and application resources. This exposure may impact data integrity or the availability of some system services.

Documentable: YES

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. The named table allows access only to session manager applications and NC-PASS applications. This USSTCP statement does not specify any type of client identifier, such as host name or IP address, so that the statement applies to all connections not otherwise controlled.

The systems programmer responsible for supporting ICS will ensure that within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications are coded only if the statements include a client identifier operand that references only secure terminals.

The systems programmer responsible for supporting ICS will ensure that any BEGINVTAM DEFAUTLAPPL statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC-PASS application as the application name.

The systems programmer responsible for supporting ICS will ensure that for systems at Z/OS Release 2.10 and above, any BEGINVTAM LUMAP statement, if used with the DEFAPPL operand and applied to unsecured terminals, specifies only a session manager

application or an NC-PASS application.

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP Data configuration file.

b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

1. Within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.
2. The USS table specified on each back stop USSTCP statement mentioned in Item (1) above is coded to allow access only to session manager applications and NC-PASS applications. This check requires Manual Review.
3. Within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.
4. Any BEGINVTAM DEFAULTAPPL statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC-PASS application as the application name. This check requires Manual Review. IBM Communications Server Data Analysis
5. Any BEGINVTAM LUMAP statement, if used with the DEFAPPL operand and applied to unsecured terminals, specifies only a session manager application or an NC-PASS application. This check requires Manual Review.

NOTE: The BEGINVTAM LINEMODEAPPL requirements will not be reviewed at this time. Further testing must be performed to determine how the CL/Supersession and NC-PASS applications work with line mode.

c) If all of the above are true, there is NO FINDING.

d) If any of the above is untrue, this is a FINDING.

Fix Text: Review the BEGINVTAM configuration statements in the PROFILE.TCPIP file. Ensure they conform to the specifications below.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

Within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.

The USS table specified on each back stop USSTCP statement mentioned above is coded to allow access only to session manager applications and NC PASS applications

Within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.

Any BEGINVTAM DEFAULTAPPL statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC PASS application as the application name

For z/OS systems, any BEGINVTAM LUMAP statement, if used with the DEFAPPL operand and applied to unsecured terminals, specifies only a session manager application or an NC PASS application.

Further explanation:

After a connection from a Telnet client to the TN3270 Telnet Server has been established, the process of session setup with a VTAM application occurs. A number of BEGINVTAM statements will be coded in a specific configuration to ensure that adequate control over access to VTAM applications is maintained.

Connections originate from secure terminals or unsecured terminals. The TN3270 Telnet Server should be configured to address these two types of connections. Terminals should meet two conditions to be considered secure. One condition involves the hardware and configuration. Secure terminals include devices that are directly attached to the host, such as 3270-type terminals coax connected to a 3174 Control Unit. They also include PCs running 3270 terminal emulation clients attached to a private LAN (i.e., a LAN without access to an external network such as the NIPRNet). The other condition involves the location of the terminals.

Secure terminals are located in areas with physical access limited to authorized personnel. Examples of terminals that are not secure are those attached via the NIPRNet or via dial-in servers. The intent of this distinction is to allow additional connection options (e.g., bypassing session manager control) to authorized personnel working in controlled access areas. These connection options may be necessary for operational control or for system recovery procedures.

The BEGINVTAM USSTCP statement can be used to specify a customized Unformatted System Services (USS) table for client connections. The USS table can provide a level of access control by restricting the commands that allow connections to VTAM applications. The USS table specified by the USSTCP statement can be the same as the one used by the SNA component of IBM Communications Server.

The BEGINVTAM DEFAULTAPPL statement can be used to specify the VTAM application to which a client is automatically connected when a session is established using a protocol other than linemode protocol.

The BEGINVTAM LUMAP statement can specify a default VTAM application using the DEFAPPL operand. This processing is similar to the DEFAULTAPPL and LINEMODEAPPL processing, except that a client identifier should be coded. When a client matches the LUMAP specification, the DEFAPPL specification overrides the DEFAULTAPPL or LINEMODEAPPL specifications.

CCI: CCI-000366

Group ID (Vulid): V-3224

Group Title: ITNT0030

Rule ID: SV-3224r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ITNT0030](#)

Rule Title: The warning banner for the TN3270 Telnet Server is not specified or properly specified.

Vulnerability Discussion: A logon banner can be used to inform users about the environment during the initial logon. In the DISA environment, logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:

The systems programmer responsible for supporting ICS will ensure that all USS tables referenced in BEGINVTAM USSTCP statements includes MSG10 text that specifies a warning logon banner.

a) Display the active started tasks executing on the domain using SDSF, or

equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP Date configuration file.

b) Ensure that all USS tables referenced in BEGINVTAM USSTCP statements include MSG10 text that specifies a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Review all USS tables referenced in BEGINVTAM USSTCP statements in the PROFILE.TCPIP file. Ensure the MSG10 text specifies a logon banner in accordance with DISA requirements. See MGG10 below:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-3226

Group Title: ITNT0050

Rule ID: SV-3226r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ITNT0050](#)

Rule Title: SSL encryption options for the TN3270 Telnet Server will be specified properly for each statement that defines a SECUREPORT or within the TELNETGLOBALS.

Vulnerability Discussion: During the SSL connection process a mutually acceptable encryption algorithm is selected by the server and client. This algorithm is used to encrypt the data that subsequently flows between the two. However, the level or strength of encryption can vary greatly. Certain configuration options can allow no encryption to be used and others can allow a relatively weak 40-bit algorithm to be used. Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECMT-2, ECTM-1

Check Content:

The systems programmer responsible for supporting ICS will ensure that a TELNETPARMS ENCRYPTION statement is coded for each statement block that defines a SECUREPORT.

The systems programmer responsible for supporting ICS will ensure that to prevent the use of null or 40-bit encryption, each TELNETPARMS ENCRYPTION statement does not specify any of the following operands: SSL_NULL_Null, SSL_NULL_MD5, SSL_NULL_SHA, SSL_RC4_MD5_EX, or SSL_RC2_MD5_EX.

a) Using SDSF or equivalent to locate the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL or the TN3270 started task if configure separately in z/OS 1.8 and above.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

b) From the ISPF Primary Option Menu use option 3.4 and review the profile configuration file and ensure the following items are in effect for the configuration statements specified in the Profile configuration file:

1. Within each TELNETPARMS block that specifies a SECUREPORT statement, an ENCRYPTION statement is also coded.
2. To prevent the use of non FIPS 140-2 encryption, each TELNETPARMS ENCRYPTION statement will specify any or all of the following operands:
 - a. SSL_3DES_SHA
 - b. SSL_AES_256_SHA
 - c. SSL_AES_128_SHA

c) If both (B)1. and (B)2. of the above are true, there is NO FINDING.

d) If either of the above is untrue, this is a FINDING.

Fix Text: The IAO will ensure the system programmer will review the SECUREPORT and TELNETPARMS ENCRYPTION statements and/or the TELNETGLOBALS statement in the PROFILE.TCPIP file. Ensuring that they conform to the requirements specified below.

The TELNETGLOBALS block may specify an ENCRYPTION statement that specifies one or more of the below cipher specifications.

Each TELNETPARMS block that specifies the SECUREPORT statement, an ENCRYPTION statement is coded with one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

To prevent the use of non FIPS 140-2 encryption, the TELNETGLOBALS block and/or each TELNETPARMS block that specifies an ENCRYPTION statement will specify one or more of the following cipher specifications:

Cipher Specifications
SSL_3DES_SHA
SSL_AES_256_SHA
SSL_AES_128_SHA

Note: Always check for the minimum allowed in FIPS 140-2.

CCI: CCI-000068

CCI: CCI-002450

Group ID (Vulid): V-3227

Group Title: ITNT0060

Rule ID: SV-3227r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ITNT0060](#)

Rule Title: SMF recording options for the TN3270 Telnet Server must be properly specified.

Vulnerability Discussion: The TN3270 Telnet Server can provide audit data in the form of SMF records. The SMF data produced provides information about individual sessions. This data includes the VTAM application, the remote and local IP addresses, and the remote and local IP port numbers. Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3

Check Content:

The systems programmer responsible for supporting ICS will ensure that the TELNETPARMS SMFINIT and SMFTERM statements are coded with the STD operand within each TELNETPARMS statement block.

a) Using SDSF or equivalent, locate the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL or the TN3270 started task if configured separately in z/OS 1.8 and above.

b) Using IBM's utility Dslist or equivalent locate the Profile configuration file and browse to review the file.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

c) Ensure the following item is in effect for the configuration statements specified in the Profile configuration file:

-The TELNETPARMS SMFINIT and SMFTERM statements are coded with the

STD operand within each TELNETPARMS statement block.

NOTE: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

d) If the above is true, there is NO FINDING.

e) If the above is untrue, this is a FINDING.

Fix Text: The system programmer responsible for the IBM Communications Server will review the TELNETPARMS SMFINIT and SMFTERM statements in the PROFILE.TCPIP file. Ensure they conform to the requirements specified below.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

The TELNETPARMS SMFINIT statement is coded with the TYPE119 operand within each TELNETPARMS statement block.

The TELNETPARMS SMFTERM statement is coded with the TYPE119 operand within each TELNETPARMS statement block.

NOTE: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

CCI: CCI-000130

Group ID (Vulid): V-3229

Group Title: IUTN0010

Rule ID: SV-3229r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IUTN0010](#)

Rule Title: The startup user account for the z/OS UNIX Telnet Server is not defined properly.

Vulnerability Discussion: The z/OS UNIX Telnet Server (i.e., otelnetd) requires a UID(0) to provide its system services. After the user enters their userid and password, otelnetd switches to the security context of the users account. Because the otelnetd account is only used until authentication is completed, there is no need to require a unique account for this function. This limits the number of privileged accounts defined to the ACP and reduces the exposure potential. Failure to properly define and control otelnetd could lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

Fix Text: Review the otelnetd startup command in the inetd.conf file and ensure the account is defined for the z/OS UNIX kernel.

The user account used at the startup of otelnetd is specified in the inetd configuration file. This account is used to perform the identification and authentication of the user requesting the session. Because the account is only used until user authentication is completed, there is no need for a unique account for this function. The z/OS UNIX kernel account can be used.

CCI: CCI-000213

Group ID (Vulid): V-3230

Group Title: IUTN0020

Rule ID: SV-3230r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IUTN0020](#)

Rule Title: Startup parameters for the z/OS UNIX Telnet Server are not specified properly.

Vulnerability Discussion: The z/OS UNIX Telnet Server (i.e., otelnetd) provides interactive access to the z/OS UNIX shell. During the initialization process, startup parameters are read to define the characteristics of each otelnetd instance. Some of these parameters have an impact on system security. Failure to specify the appropriate command options could result in degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the otelnetd startup command includes the options -D login and -c 900, where:

-D login indicates that messages should be written to the syslogd facility for login and logout activity
-c 900 indicates that the Telnet session should be terminated after 15 minutes of inactivity.

The systems programmer responsible for supporting ICS will ensure that the otelnetd startup command does not include the option -h, where:

-h indicates that the logon banner should not be displayed.

a) Using Vanguard Administrator UNIX File Manager option 14. User the CD command to change to the etc directory and the browse the file /etc/inetd.conf

b) Ensure the following items are in effect for the otelnetd startup command:

1. Option -D login is included on the otelnetd command.
2. Option -c 900 is included on the otelnetd command.

NOTE: 900 indicates a session timeout value of 15 minutes and is currently the maximum value allowed.

3. Option -h is not included on the otelnetd command.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Review the startup parameters in the inetd.conf file for otelnetd and ensure they conform to the specifications below.

The otelnetd startup command includes the options -D login and -c 900, where:

-D login indicates that messages should be written to the syslogd facility for login and logout activity

-c 900 indicates that the Telnet session should be terminated after 15 minutes of inactivity.

NOTE: The 900 is the maximum value; any value between 1 and 900 is acceptable.

The otelnetd startup command should not include the option -h, where:

-h indicates that the logon banner should not be displayed.

CCI: CCI-001133

Group ID (Vulid): V-3231

Group Title: IUTN0030

Rule ID: SV-3231r2_rule

Severity: CAT II

Rule Version (STIG-ID): [IUTN0030](#)

Rule Title: The warning banner for the z/OS UNIX Telnet Server is not specified or not properly specified.

Vulnerability Discussion: A logon banner can be used to inform users about the environment during the initial logon. Logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Documentable: YES

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(IUTN0030)

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IUTN0030)

- PDIx(IUTN0030) Note: Created when sites have multiple TCP/IP and FTP started task procedures.

NOTE: Additional Analysis will be required for the above file.

b) Ensure the /etc/banner file contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

Fix Text: Review the /etc/banner file and ensure the text specifies a logon banner in accordance with DISA requirements.

DOD requires that a logon warning banner be displayed. Although the z/OS UNIX Telnet Server does not support the display of a message before the logon prompt, it is possible to display a message immediately after logon.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-3232

Group Title: IUTN0040

Rule ID: SV-3232r3_rule

Severity: CAT II

Rule Version (STIG-ID): [IUTN0040](#)

Rule Title: HFS objects for the z/OS UNIX Telnet Server will be properly protected.

Vulnerability Discussion: HFS directories and files of the z/OS UNIX Telnet Server provide the configuration and executable properties of this product. Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(IUTN0040)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ZUTN0040)

The HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table. If the guidance is true, this is not a finding.

z/OS UNIX TELNET Server HFS Object Security Settings

| File | Permission Bits | User Audit Bits |
|---------------------|-----------------|-----------------|
| /usr/sbin/otelnetsd | 1740 | fff |
| /etc/banner | 0744 | faf |

NOTE:

The /usr/sbin/otelnetsd object is a symbolic link to /usr/lpp/tcpip/sbin/otelnetsd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwX | (least restrictive) |
| 6 | rw- | |
| 3 | -wX | |
| 2 | -w- | |
| 5 | r-X | |
| 4 | r-- | |
| 1 | --X | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

- f log for failed access attempts
- a log for failed and successful access
- no auditing

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the z/OS UNIX Telnet Server. Ensure they conform to the specifications below:

z/OS UNIX TELNET Server HFS Object Security Settings

| File | Permission Bits | User Audit Bits |
|--------------------|-----------------|-----------------|
| /usr/sbin/otelneta | 1740 | fff |
| /etc/banner | 0744 | faf |

NOTE:

The /usr/sbin/otelneta object is a symbolic link to /usr/lpp/tcpip/sbin/otelneta. The permission and user audit bits on the target of the symbolic link must have the required settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwX | (least restrictive) |
| 6 | rw- | |
| 3 | -wX | |
| 2 | -w- | |
| 5 | r-X | |
| 4 | r-- | |
| 1 | --X | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/otelneta
chaudit rwX=f /usr/lpp/tcpip/sbin/otelneta
chmod 0744 /etc/banner
chaudit w=sf,rX+f /etc/banner
```

CCI: CCI-000213

CCI: CCI-000225

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-7516

Group Title: ZCIC0010

Rule ID: SV-7978r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZCIC0010](#)

Rule Title: CICS system data sets are not properly protected.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications. Unauthorized access to CICS system data sets (i.e., product, security, and application libraries) could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(CICSRPT)

Since it is possible to have multiple CICS regions running on an LPAR, it is recommended that you go into the z/OS STIG Addendum and fill out all the information in the "CICS System Programmers Worksheet" for each CICS region running on your LPAR. It is recommended that you save this information for any other CICS vulnerabilities that will require it.

b) WRITE and/or ALLOCATE access to CICS system data sets is restricted to systems programming personnel.

c) If (b) is true, there is NO FINDING.

d) If (b) is untrue, this is a FINDING.G.

d) If (b) is untrue, this is a FINDING.

Fix Text: Review the access authorizations for CICS system data sets for each region. Ensure they conform to the specifications below:

A CICS environment may include several data set types required for operation. Typically they are CICS product libraries, which are usually included in the STEPLIB concatenation but may be found in DD DFHRPL. CICS system data sets that can be identified with DFH DD statements, other product system data sets, and application program libraries. Restrict alter and update access to CICS program libraries and all system data sets to systems programmers only. Other access must be documented and approved by the IAO. The site may determine access to application data sets included in the DD DFHRPL and CICS region startup JCL according to need. Ensure that procedures are established; documented, and followed that prevents the introduction of unauthorized or untested application programs into production application systems.

CCI: CCI-001499

Group ID (Vulid): V-251

Group Title: ZCIC0020

Rule ID: SV-7528r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZCIC0020](#)

Rule Title: Sensitive CICS transactions are not protected in accordance with security requirements.

Vulnerability Discussion: Sensitive CICS transactions offer the ability to circumvent transaction level controls for accessing resources under CICS. These transactions must be protected so that only authorized users can access them. Unauthorized use can result in the compromise of the confidentiality, integrity, and availability of the operating system or customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(TRANS)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010..

b) Browse the data set allocated by the ACF2PARM DD statement in each CICS startup procedure. Determine the resource type for transactions. Example:

CICSKEY OPTION=VALIDATE,TYPE=resource type, RESOURCE=TRANS

c) Ensure the following items are in effect for all CICS transactions for each resource type:

NOTE: Authorized personnel include systems programming and security staffs. Additional guidance regarding authorized personnel for specific transactions is included in this z/OS STIG Addendum. For example, CEMT SPI provides a broader use of this sensitive transaction by restricting execution to inquiries.

1) Transactions, listed in tables CICS CATEGORY 2 CICS AND OTHER PRODUCT TRANSACTIONS and CICS CATEGORY 4 COTS-SUPPLIED SENSITIVE TRANSACTIONS, in the z/OS STIG Addendum, are restricted to authorized personnel.

Note: The exception to this is the CEOT and CSGM transactions, which can be made available to all users.

Note: The exception to this is the CWBA transaction, can be made available to the CICS Default user.

Note: The transactions beginning with "CK" apply to regions running WebSphere MQ.

Note: Category 1 transactions are internally restricted to CICS region userids.

d) If (c) is true for all CICS regions, there is NO FINDING.

e) If (c) is untrue for any CICS region, this is a FINDING.

Fix Text: The IAO will ensure that each CICS region is associated with a unique userid and that userid is properly defined.

Develop a plan to implement the required changes.

1. Most transactions are protected in groups. An example would be "KT2" which would contain all Category 2 transactions. KT2 is defined to ACF2 as a resource and contains all the Category 2 transactions.

An example of how to implement this within ACF2 is shown here:

```
$KEY(CEMT) TYPE(KT2)
```

```
UID(syspau) ALLOW
```

```
UID(*) PREVENT
```

2. Transactions groups should be defined and permitted in accordance with the CICS Transaction tables listed in the z/OS STIG Addendum.

CCI: CCI-000213

Group ID (Vulid): V-302

Group Title: ZCIC0030

Rule ID: SV-7530r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZCIC0030](#)

Rule Title: CICS System Initialization Table (SIT) parameter values must be specified in accordance with proper security requirements.

Vulnerability Discussion: The CICS SIT is used to define system operation and configuration parameters of a CICS system. Several of these parameters control the security within a CICS region. Failure to code the appropriate values could result in unexpected operations and degraded security. This exposure may result in unauthorized access impacting the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Gather from your CICS programmer the list of JCL used to start each CICS region. Generally these will be found in a proclib member.

Refer to the information gathered from the CICS Systems Programmer's Worksheet in the Preliminary Information Worksheets.

Refer to the CICS region SYSLOG - (Alternate source of SIT parameters). Be sure to process DFHSIT based on the order specified in Note 2

b) Ensure the following CICS System Initialization Table (SIT) parameter settings are specified for each CICS region:

The system initialization parameters are processed in the preceding order, with later system initialization parameter values overriding those specified earlier

1. SEC=YES

If SEC is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the external security setting in bold:

X 80 EQU B 10000000 EXTERNAL SECURITY REQUESTED
X 40 EQU B 01000000 RESOURCE PREFIX REQUIRED
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required

X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check

2. DFLTUSER=CICSUSER | userid

If DFLTUSER is not coded in the CICS region startup JCL, go to offset x 118 from the beginning on the SIT dump (record sequence number - 6) for a length of 8 bytes. The value will be the CICS default userid.

3. XUSER=YES

If XUSER is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the surrogate user checking setting in bold:

X 80 EQU B 10000000 EXTERNAL SECURITY REQUESTED
X 40 EQU B 01000000 RESOURCE PREFIX REQUIRED
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check

4. SNSCOPE=NONE | CICS | MVSIMAGE | SYSPLEX

If SNSCOPE is not coded in the CICS region startup JCL, go to offset x 124 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the signon scope byte flag. Below are the hex settings for this flag:

X 01 EQU 1 SIGNON SCOPE = NONE
X 02 EQU 2 SIGNON SCOPE = CICS
X 03 EQU 3 SIGNON SCOPE = MVSIMAGE
X 04 EQU 4 SIGNON SCOPE = SYSPLEX

NOTE: SNSCOPE=NONE is only allowed with test/development regions.

5. XTRAN=YES | ssrrTRN | classname

If XTRAN is not coded in the CICS region startup JCL, go to offset x CA from the beginning on the SIT dump (record sequence number - 6) for a length of 7 bytes. The value will be the resource class name used for that region. If XTRAN=YES is coded, c CICSTRN will be present.

6. SECPRFX=YES

If SECPRFX is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the resource prefixing setting in bold:

X 80 EQU B 10000000 EXTERNAL SECURITY REQUESTED
X 40 EQU B 01000000 RESOURCE PREFIX REQUIRED
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check

NOTE 1: If XTRAN=ssrrTRN is specified, resource prefixing (e.g. SECPRFX=YES) is not required to be enabled. Also, CICS regions cannot share the same resource class if resource prefixing is not active.

NOTE 2: CICS system initialization parameters are specified in the following ways:

- (a) In the system initialization table, loaded from a library in the STEPLIB concatenation of the CICS startup procedure.
- (b) In the PARM parameter of the EXEC PGM=DFHSIP statement of the CICS startup procedure.
- (c) In the SYSIN data set defined in the startup procedure (but only if SYSIN is coded in the PARM parameter).

c) If the SIT parameters are defined as specified in (b) for each CICS region, there is NO FINDING.

d) If any SIT parameter is not defined as specified in (b) for a CICS region, this is a

FINDING.

Fix Text: Ensure that CICS System Initialization Table (SIT) parameter values are specified using the following guidance.

The system initialization parameters are processed in the following order, with later system initialization parameter values overriding those specified earlier. CICS system initialization parameters are specified in the following ways:

In the system initialization table, loaded from a library in the STEPLIB concatenation of the CICS startup procedure.

In the PARM parameter of the EXEC PGM=DFHSP statement of the CICS startup procedure.

In the SYSIN data set defined in the startup procedure (but only if SYSIN is coded in the PARM parameter).

SEC=YES - If SEC is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag.

```
X 80 EQU B 10000000 External Security Requested <<===  
X 40 EQU B 01000000 Resource Prefix Required  
X 10 EQU B 00010000 RACLIST class APPCLU required  
X 08 EQU B 00001000 ESM INSTLN data is required  
X 04 EQU B 00000100 Surrogate User Checking required  
X 02 EQU B 00000010 Always enact resource check  
X 01 EQU B 00000001 Always enact command check
```

DFLTUSER=<parameter> - If DFLTUSER is not coded in the CICS region startup JCL, go to offset x 118 from the beginning on the SIT dump (record sequence number - 6) for a length of 8 bytes. The value will be the CICS default userid.

XUSER=YES - If XUSER is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag.

```
X 80 EQU B 10000000 External Security Requested  
X 40 EQU B 01000000 Resource Prefix Required  
X 10 EQU B 00010000 RACLIST class APPCLU required  
X 08 EQU B 00001000 ESM INSTLN data is required  
X 04 EQU B 00000100 Surrogate User Checking required <<===  
X 02 EQU B 00000010 Always enact resource check  
X 01 EQU B 00000001 Always enact command check
```

SNSCOPE=NONE|CICS|MVSIMAGE|SYSPLEX

If SNSCOPE is not coded in the CICS region startup JCL, go to offset x 124 from the beginning on the SIT dump (record sequence number - 6) for a length of 1.

This is the signon scope byte flag. Ensure that users cannot sign on to more than one CICS production region within the scope of a single CICS region, a single z/OS image, or a sysplex. Below are the hex settings for this flag:

X 01 EQU 1 SIGNON SCOPE = NONE
X 02 EQU 2 SIGNON SCOPE = CICS
X 03 EQU 3 SIGNON SCOPE = MVSIMAGE
X 04 EQU 4 SIGNON SCOPE = SYSPLEX

Note: SNSCOPE=NONE is only allowed with test/development regions.

XTRAN=YES|ssrrTRN - If XTRAN is not coded in the CICS region startup JCL, go to offset x CA from the beginning on the SIT dump (record sequence number - 6) for a length of 7 bytes. The value will be the resource class name used for that region. If XTRAN=YES is coded, c CICSTRN will be present.

SECPRFX=YES - If SECPRFX is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the resource prefixing setting bolded:

X 80 EQU B 10000000 External Security Requested
X 40 EQU B 01000000 Resource Prefix Required <<===
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check

Note: If XTRAN=ssrrTRN is specified, resource prefixing (e.g., SECPRFX=YES) is not required to be enabled. Also, CICS regions cannot share the same resource class if resource prefixing is not active.

CCI: CCI-000366

Group ID (Vulid): V-44

Group Title: ZCIC0040

Rule ID: SV-7532r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZCIC0040](#)

Rule Title: CICS region logonid(s) must be defined and/or controlled in accordance with the security requirements.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications.

Improperly defined or controlled CICS userids (i.e., region, default, and terminal users) may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CICSPROC)

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(LOGONIDS)

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010.

b) Ensure the following items are in effect for each CICS region logonid:

- 1) A unique logonid is associated with the CICS region.
 - 2) The CICS region logonid has the ACF2CICS, MUSASS, and NO-SMC attributes specified.
- NOTE: The ACF2CICS privilege will be restricted to CICS region logonids only.
- 3) If CICS region submits jobs on behalf of its users, the JOBFROM attribute is specified.
 - 4) If CICS region has a requirement to update information in the ACF2 database, the MUSUPDT attribute is specified.
 - 5) Not granted the ACF2 NON-CNCL privilege.
 - 6) No access to interactive on-line facilities (e.g., TSO) other than CICS.

c) If (b) are true, this is not a finding.

d) If (b) is untrue, this is a finding.

Fix Text: The IAO will ensure that each CICS region is associated with a unique userid and that userid is properly defined.

Review all CICS region, default, and end-user userids to ensure they are defined and controlled as required.

Ensure that the following is defined for each CICS region:

- 1) A unique userid is defined.

Use the ACF2 insert command to accomplish this. A sample command is provided here:

INSERT <cicsregionid> NAME('STC, CICS Region') JOBFROM MUSASS NO-SMC STC ACF2CICS

CCI: CCI-000764

Group ID (Vulid): V-7119

Group Title: ZCIC0041

Rule ID: SV-7536r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZCIC0041](#)

Rule Title: CICS default logonid(s) must be defined and/or controlled in accordance with the security requirements.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications. An improperly defined or controlled CICS default userid may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CICSPROC)

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(LOGONIDS)
- ACF2CMDS.RPT(RESOURCE)

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010.

b) Ensure the following items are in effect for the CICS default logonid(s) (i.e., Browse the ACF2PARM DD statement for DEFAULT TERMINAL=<parameter> and DEFAULT NONTERMINAL=nnnnnnnn):

- 1) Not granted the ACF2 NON-CNCL privilege.
- 2) No access to interactive on-line facilities (e.g., TSO) other than CICS.
- 3) IDLE(15) field is set to 15 minutes.

4) A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.

5) Restricted from accessing all data sets and resources with the following exceptions:

- (a) Non-restricted CICS transactions (e.g., CESF, CESN, good morning transaction, etc.)
- (b) If applicable, resources necessary to operate in an intersystem communication (ISC) environment (i.e., LU6.1, LU6.2, and MRO)
- c) If all items in (b) are true, this is not a finding.
- d) If any item in (b) is untrue, this is a finding.

Fix Text: Ensure that the default CICS user is restricted and properly defined.

Ensure the following items are in effect for the CICS default logonid(s) (i.e., Browse the ACF2PARM DD statement for DEFAULT TERMINAL=<parameter> and DEFAULT NONTERMINAL=nnnnnnnn):

Not granted the ACF2 NON-CNCL privilege.
Use the ACF2 LIST command to display the default CICS userid.

Example:
SET LID
LIST CICS
CHANGE CICS NONON-CNCL

No access to interactive online facilities (e.g., TSO) other than CICS.

Use the ACF2 LIST command to display the default CICS userid.

Example:
SET LID
LIST CICS
CHANGE CICS NOTSO

IDLE(15) field is set to 15 minutes, up to 30 with justification.

Use the ACF2 LIST command to display the default CICS userid.

Example:

```
SET LID
LIST CICS
CHANGE CICS IDLE(15) up to 30 with justification
```

Restricted from accessing all data sets and resources with the following exceptions:

Non-restricted CICS transactions (e.g., CESF, CESN, good morning transaction, etc.)

If applicable, resources necessary to operate in an intersystem communication (ISC) environment (i.e., LU6.1, LU6.2, and MRO)

Use the ACF2 ACFRPTX or ACFRPTXR reports to verify if the CICS default userid has access to any resources or datasets.

CCI: CCI-000764

Group ID (Vulid): V-7120

Group Title: ZCIC0042

Rule ID: SV-7540r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZCIC0042](#)

Rule Title: CICS logonid(s) do not have time-out limit set to 15 minutes.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications. Improperly defined or controlled CICS region userids may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

RACF provides the PROPCNTL class to prevent userids such as the CICS region userid from being propagated/used by unauthorized userids.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(LOGONIDS)

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010.

Note: Any logonid that does not have an IDLE value specified will obtain its IDLE value from the default value set in ZCIC0041. Any logonid that specifies an IDLE value must meet the requirements specified below.

b) For all logonids with the CICS attribute that have IDLE(15) specified this is not a finding.

NOTE: If the time-out limit is greater than 15 minutes, and the system is processing unclassified information, review the following items. If any of these is true, this is not a finding.

If a session is not terminated, but instead is locked out after 15 minutes of inactivity, a process must be in place that requires user identification and authentication before the session is unlocked. Session lock-out will be implemented through system controls or terminal screen protection.

A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the ISSM. The ISSM will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.

The ISSM may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:

The time-out exception cannot exceed 60 minutes.

A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site IAM. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.). The requirement must be revalidated on an annual basis.

c) If the MULTSIGN option in the logonid record field is restricted to test or development use, this is not a finding.

Fix Text: Ensure that all userids with a CICS segment have the TIMEOUT parameter set to 15 minutes.

Ensure that all LIDs authorized to access a CICS facility restrict MULTSIGN to test and development use.

Examples:

SET LID

LIST CICS

CHANGE CICS IDLE(15)

CCI: CCI-000057

Group ID (Vulid): V-6900

Group Title: ZFEP0011

Rule ID: SV-7195r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZFEP0011](#)

Rule Title: All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 1, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

* Item 1: Documents and procedures restricting access to the hardware components of the FEPs.

b) If the hardware components of the FEPs are located in secure locations, there is NO FINDING.

c) If the hardware components of the FEPs are not located in secure locations, this is a FINDING.

Fix Text: Ensure that hardware components of the FEPs are protected as specified below:

Physical security is the first level of security control for the FEPs. Install all hardware components of the FEPs in secure locations where they cannot be stolen, damaged, or disturbed. Make sure that FEP hardware is located in a secure area with limited access to authorized personnel.

CCI: CCI-000933

Group ID (Vulid): V-6901

Group Title: ZFEP0012

Rule ID: SV-7196r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZFEP0012](#)

Rule Title: Procedures are not in place to restrict access to FEP functions of the service subsystem from operator consoles (local and/or remote), and to restrict access to the diskette drive of the service subsystem.

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the Front End Processor (FEP) Protection Worksheet, Items 1-4, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

- * Item 1: Documents and procedures restricting access to the hardware components of the FEPs.

- * Item 2: Documents and procedures restricting access to the functions of the service subsystem from the control panel.

- * Item 3: Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).

- * Item 4: Documents and procedures restricting access to the diskette drive of the service subsystem.

b) If a procedure is in place to restrict access to the functions of the service subsystem, there is NO FINDING.

c) If a procedure is in place to restrict access to the functions of the service subsystem from operator consoles (local and/or remote), there is NO FINDING.

d) If a procedure is in place to restrict access to the diskette drive of the service subsystem, there is NO FINDING.

e) If no procedure exists for any of the above functions of the service subsystem and FEP resources, this is a FINDING.

Fix Text: Ensure that all hardware components of the FEPs are protected as described below and supporting documentation procedures exist for each item:

1. Documents and procedures restricting access to the hardware components of the FEPs.
2. Documents and procedures restricting access to the functions of the service subsystem from the control panel.
3. Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).
4. Documents and procedures restricting access to the diskette drive of the service subsystem.

CCI: CCI-000004

Group ID (Valid): V-6902

Group Title: ZFEP0013

Rule ID: SV-7197r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZFEP0013](#)

Rule Title: A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program).

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

Responsibility: N/A

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 6, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

* Item 6: Documents and procedures regarding the NCP load and dump processes.

b) If a procedure is in place relative to the NCP load and dump processes, there is NO FINDING.

c) If no procedure is in place relative to the NCP load and dump processes, this is a

FINDING.

Fix Text: If documented procedures for loading and dumping the FEP NCP (Network Control Program) are not available. Create a procedure document for dumping and loading the FEP and make sure that they are available to the IAO and to authorized personnel responsible to perform these functions.

CCI: CCI-000504

Group ID (Vulid): V-6903

Group Title: ZFEP0014

Rule ID: SV-7198r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZFEP0014](#)

Rule Title: An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor).

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 8, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

* Item 8: All documents and procedures that apply to FEP operations including network management, FEP initialization, IPL, shutdown, NCP dumping, backup, and recovery.

b) If a log is in place to keep track of all hardware upgrades and software changes, there is NO FINDING..

c) If a log is in place to keep track of all hardware upgrades and software changes, there is NO FINDING.

Fix Text: The systems programmer will see that a a log of all hardware and software upgrades/changes has been created for auditing purposes and problem tracking. All changes and upgrades will be logged.

CCI: CCI-000318

Group ID (Vulid): V-6904

Group Title: ZFEP0015

Rule ID: SV-7199r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZFEP0015](#)

Rule Title: NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE and/or ALLOCATE access to appropriate personnel.

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

- a) Reference data from item 4 of the Z/OS Systems Programmer s Worksheet, located in U_zOS_STIG_INSTRUCTION.doc to locate the JES2 proclibs.
- b) Search the JES2 proclibs for the member that executes program ISTINM01. These data sets are used for the FEP at the site; if the domain does not have a FEP the collection of these data sets can be bypassed. Review the VTAM procedure for load and dump data sets for the FEP. Use ISPF/PDF option 3.4 data set name list to enter ****.*NCP***. Enter the names of the above datasets in a sequential dataset. Make note of the dataset name for item C below.
- c) From Analyzer main Menu, go to B, Sensitive Critical Data Sets Analysis , enter R to the left of User defined list . Enter the name of the sequential dataset created from above to the right of the **===>**. Press enter.
- d) Review the User defined list shown. If there are entries in the displayed list that have either R, N, E, or W in the M column, there is a FINDING for NCP data sets allowing inappropriate access.
- e) Review each data set shown in the User defined list by entering VRC under the Opt heading. Check the access to these data set rules to ensure they do not allow UPDATE and/or ALTER access to authorized personnel (e.g., Z/OS

systems programming personnel). If any allow UPDATE or ALTER access, this is a FINDING

Fix Text: Identify Names of the following data sets used for installation and in development/production environments:

- NCP system data sets
- NCP source definition data sets
- NCP load modules
- NCP host dump data sets
- NCP utility programs

Have the IAO validate that they are properly protected by the ACP. And that only authorized personnel are permitted UPDATE and/or ALLOCATE access (e.g., z/OS systems programming personnel).

CCI: CCI-001499

Group ID (Vulid): V-6905

Group Title: ZFEP0016

Rule ID: SV-7200r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZFEP0016](#)

Rule Title: A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem.

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, IAAC-1

Check Content:

a) Refer to the Front End Processor (FEP) Protection Worksheet, Items 1-4, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

* Item 1: Documents and procedures restricting access to the hardware components of the FEPs.

* Item 2: Documents and procedures restricting access to the functions of the

service subsystem from the control panel.

* Item 3: Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).

* Item 4: Documents and procedures restricting access to the diskette drive of the service subsystem.

b) If a password control is in place to restrict access to the service subsystem via the operator consoles (local and/or remote), there is NO FINDING.

a) If a key-lock switch is used to protect the modem supporting the remote console of the service subsystem, there is NO FINDING.

b) If no procedure exists for any of the above functions of the service subsystem and FEP resources, this is a FINDING.

Fix Text: If any of the below procedures are not in place, than correct the situation by documenting the missing procedure(s).

The systems programmer should validate that Control authorization to use service subsystem console (local or remote) by FEP internal security control through password validation. Restrict access to these passwords to the absolutely minimum number of necessary personnel. Use of vendor default passwords is prohibited. Assign different passwords for the local and remote consoles. Disconnect the local/remote console after three unsuccessful attempts to log on. Passwords used by vendor (COMTEN, IBM, CNT, or AMDAHL) service personnel will be changed after any maintenance is done. All passwords will be changed every 90 days. Restrict permission to change passwords only to authorized personnel.

Use a key lock switch on the modem supporting the remote console of the service subsystem to prevent unauthorized access. The key lock switch is only open for scheduled and authorized remote access.

CCI: CCI-000213

Group ID (Vulid): V-6919

Group Title: ZJES0021

Rule ID: SV-7323r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0021](#)

Rule Title: JES2 input sources are not controlled in accordance with the proper security requirements.

Vulnerability Discussion: JES2 input sources provide a variety of channels for job submission. Failure to properly control the use of these input sources could result in unauthorized submission of work into the operating system. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(JESINPUT)
- ACF2CMDS.RPT(RESOURCE) Alternate report
- ACF2CMDS.RPT(ACFGSO)

Refer to the following report produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

b) Review the ACFGSO report. If CLASMAP defines JESINPUT as TYPE(INP), there is NO FINDING.

NOTE: If CLASMAP defines JESINPUT as anything other than TYPE(INP), replace INP below with the appropriate three letters.

c) Review the following resources in the JESINPUT resource class (i.e., TYPE(INP)):

INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.- (spool offload receiver)
Rnnnn.- (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

NOTE: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be defined.

NOTE 1: Nodename is the NAME parameter in the NODE statement. Review the NJE node definitions by searching for NODE(in the JES2 parameters.

NOTE 2: OFFn, where n is the number of the offload receiver. Review the spool offload receiver definitions by searching for OFF(in the JES2 parameters.

NOTE 3: Rnnnn, where nnnn is the number of the remote workstation. Review the RJE node definitions by searching for RMT(in the JES2 parameters.

NOTE 4: RDRnn, where nn is the number of the reader. Review the reader definitions by searching for RDR(in the JES2 parameters.

d) Ensure the following items are in effect:

- 1) The CLASMAP record defines the JESINPUT resource class to TYPE(INP).
- 2) The resources mentioned in (b) are protected by generic and/or fully qualified rules defined to the JESINPUT resource class.
- 3) A default access of PREVENT is specified for all resources.

NOTE: A default access of READ is allowed for input sources that are permitted to submit jobs for all users. No guidance on which input sources are appropriate for a default access of READ. However, common sense should prevail during the analysis. For example, a default access of READ would typically be inappropriate for RJE, NJE, offload, and STC input sources.

- e) If all of the items in (b) and (d) are true, there is NO FINDING.
- f) If any item in (b) or (d) is untrue, this is a FINDING.

Fix Text: Review the following resources in the JESINPUT resource class:

INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.* (spool offload receiver)
Rnnnn (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

NOTE: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be defined.

NOTE 1: Nodename is the NAME parameter in the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report.

NOTE 2: OFFn, where n is the number of the offload receiver. Review the JES2 parameters for spool offload receiver definitions by searching for OFF(in the report.

NOTE 3: Rnnnn, where nnnn is the number of the remote workstation. Review the JES2 parameters for RJE node definitions by searching for RMT(in the report.

NOTE 4: RDRnn, where nn is the number of the reader. Review the JES2 parameters for reader definitions by searching for RDR(in the report.

c) Ensure the following items are in effect:

- 1) The JESINPUT resource class is active.

2) The resources mentioned in (b) are protected by generic and/or fully qualified profiles defined to the JESINPUT resource class.

3) UACC(NONE) is specified for all resources.

NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs for all users. Currently, there is no guidance on which input sources are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, offload, and STC input sources.

Examples:

```
setr classact(jesinput)
setr generic(jesinput)
rdef jesinput intrdr uacc(none) owner(admin) audit(failures(read) success(update)) data('Per SRR PDI ZJES0021')
pe intrdr cl(jesinput) id(<syspau>)
pe intrdr cl(jesinput) id(*) /* all users */
```

CCI: CCI-000213

CCI: CCI-001310

Group ID (Vulid): V-6920

Group Title: ZJES0022

Rule ID: SV-74863r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0022](#)

Rule Title: JES2 input sources must be properly controlled.

Vulnerability Discussion: JES2 input sources provide a variety of channels for job submission. Failure to properly control the use of these input sources could result in unauthorized submission of work into the operating system. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: N/A

IAControls: N/A

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(JESINPUT)

Verify that the accesses for JESINPUT resources are restricted. If the following guidance is true, this is not a finding.

___ The ACF2 resources and/or generic equivalent are defined with a default access of PREVENT.

___ The ACF2 resources and/or generic equivalent identified below will be defined with access restricted to the appropriate personnel:

INTRDR
nodename
OFFn.*
OFFn.JR
OFFn.SR
Rnnnn.RDm
RDRnn
STCINRDR
TSUINRDR and/or TSOINRDR

NOTE: Use common sense during the analysis. For example, access to the offload input sources should be limited to systems personnel (e.g., operations staff).

Fix Text: Verify with the ISSO that access authorization for resources defined to the JESINPUT resource class is restricted to the appropriate personnel

Grant read access to authorized users for each of the following input sources:

INTRDR
nodename
OFFn.*
OFFn.JR
OFFn.SR
Rnnnn.RDm
RDRnn
STCINRDR
TSUINRDR and/or TSOINRDR

The resource definition will be generic if all of the resources of the same type have identical access controls (e.g., if all off load receivers are equivalent). The default access will be NONE except for sources that are permitted to submit jobs for all users. Those resources may be defined as either NONE or READ.

CCI: CCI-000213

Group ID (Vulid): V-6921

Group Title: ZJES0031

Rule ID: SV-7327r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0031](#)

Rule Title: JES2 output devices are not controlled in accordance with the proper security requirements.

Vulnerability Discussion: JES2 output devices provide a variety of channels to which output can be processed. Failure to properly control these output devices could result in unauthorized personnel accessing output. This exposure may compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.

b) Review the local printer definitions by searching for PRT(or PRINTER in the member.

c) Review the local card definitions by searching for PUN(or PUNCH in the member.

d) Review the remote workstation printer definitions by searching for .PR in the member.

e) Review the remote workstation punch definitions by searching for .PU in the member.

f) Use the list of NJE nodes from ZJES012 and the list of offload receivers from ZJES0021.

g) From Administrator main Menu, select option 9 Analyzer. Press <ENTER>

h) From Analyzer main menu, select 4 Batch Reports. Press <ENTER>

i) From Batch Reports menu, select F Subsystem Name Table Analysis. Press <ENTER>

j) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press <ENTER>

k) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press <ENTER>

l) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

m) Review the output. Note that the first entry in the report is the JES2 subsystem name and is typically JES2. This will be used in step p.

n) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>

o) Select option 4 General Resource Profile

p) In all profile names, replace JES2 with the JES2 subsystem name determined in step m.

q) On the General Resources Reports panel, enter JES2.** in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>

r) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

s) Save the output for use in the JES2.** (backstop profile) check.

t) On the General Resources Reports panel, enter JES2.LOCAL.OFF%.* in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>

u) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

v) Save the output for use in the JES2.LOCAL.OFFn.*, JES2.LOCAL.OFFn.ST, and JES2.LOCAL.OFFn.JT (spool offload related) checks.

w) On the General Resources Reports panel, enter JES2.LOCAL.PRT% in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.

Press <ENTER>

x) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

y) Save the output for use in the JES2.LOCAL.PRTn ((local printer)) checks.

z) On the General Resources Reports panel, enter JES2.LOCAL.PUN% in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>

aa) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

bb) Save the output for use in the JES2.LOCAL.PUNn (local punch) check.

cc) Using the node list mentioned in step f, on the General Resources Reports panel, enter nodename in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>

dd) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

ee) Save the output for use in the nodename (NJE node) check.

ff) Repeat step u through w for each nodename in the list

gg) On the General Resources Reports panel, enter JES2.RJE.R% % % .P* in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>

hh) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

ii) Save the output for use in the JES2.RJE.Rnnnn.PRm and JES2.RJE.Rnnnn.PUm (remote printer and punch) checks.

jj) From Administrator main Menu, select option 2 Security Server Commands. Press <ENTER>

kk) From the VRC main menu, select option 5 SETROPTS. Press <ENTER>

ll) Under Class Options, enter E after CDT Classes. Press <ENTER>

mm) Enter L WRITER on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen and save it for the class active check.

nn) Review the following resources in the WRITER resource class where JES2 is the name of the JES2 subsystem:

- * JES2.** (backstop profile) review output from step s.

- * JES2.LOCAL.OFFn.* (spool offload transmitter) review output from step v.

- * JES2.LOCAL.OFFn.ST (spool offload SYSOUT transmitter) review output from step v.

- * JES2.LOCAL.OFFn.JT (spool offload job transmitter) review output from step v.

- * JES2.LOCAL.PRTn (local printer) review output from step q.

- * JES2.LOCAL.PUNn (local punch) review output from step t.

- * JES2.NJE.nodename (NJE node) review output from step ee.

- * JES2.RJE.Rnnnn.PRm (remote printer) review output from step ii.

- * JES2.RJE.Rnnnn.PUm (remote punch) review output from step ii.

NOTE: If any of these are not found, that resource in the WRITER resource class does not have to be defined.

oo) Ensure the following items are in effect:

5. The WRITER resource class is active (obtained in step mm).

6. The resources mentioned in step nn are protected by generic and/or fully qualified profiles defined to the WRITER resource class.

7. UACC(NONE) is specified for all resources.

8. NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs for all users. Currently, the Z/OS STIG provides no guidance on which input sources are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, offload, and STC input sources.

pp) If all of the items mentioned in (oo) are true, there is NO FINDING.

qq) If any of the items mentioned in (oo) is untrue, this is a FINDING.

Fix Text: WRITER Resource Definitions

Review the following resources in the WRITER resource class:

| | |
|--------------------|------------------------------------|
| JES2.** | (backstop profile) |
| JES2.LOCAL.OFFn.* | (spool offload transmitter) |
| JES2.LOCAL.OFFn.ST | (spool offload SYSOUT transmitter) |
| JES2.LOCAL.OFFn.JT | (spool offload job transmitter) |
| JES2.LOCAL.PRTn | (local printer) |
| JES2.LOCAL.PUNn | (local punch) |
| JES2.NJE.nodename | (NJE node) |
| JES2.RJE.Rnnnn.PRm | (remote printer) |
| JES2.RJE.Rnnnn.PUm | (remote punch) |

NOTE 1: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

NOTE 2: OFFn, where n is the number of the offload transmitter. Determine the numbers by searching for OFF(in the JES2 parameters.

NOTE 3: PRTn, where n is the number of the local printer. Determine the numbers by searching for PRT(in the JES2 parameters.

NOTE 4: PUNn, where n is the number of the local card punch. Determine the numbers by searching for PUN(in the JES2 parameters.

NOTE 5: Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report.

NOTE 6: Rnnnn.PRm, where nnnn is the number of the remote workstation and m is the number of the printer. Determine the numbers by searching for .PR in the JES2 parameters.

NOTE 7: Rnnnn.PUm, where nnnn is the number of the remote workstation and m is the number of the punch. Determine the numbers by searching for .PU in the JES2 parameters.

c) Ensure the following items are in effect:

- 1) The WRITER resource class is active.
- 2) The profile JES2.** is defined to the WRITER resource class with a UACC(NONE).
- 3) The other resources mentioned in (b) are protected by generic and/or fully qualified profiles defined to the WRITER resource class with UACC(NONE).

NOTE: UACC(READ) is allowed for output destinations that are permitted to route output for all users. Currently, there is no guidance on which output destinations are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, and offload output destinations.

Examples:

```
setr classact(writer)
setr gencmd(writer) generic(writer)
setr raclist(writer)
RDEF WRITER JES2.** owner(admin) AUDIT(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.** owner(admin) AUDIT(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.JT owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.ST owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PRT* owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PUN* owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.NJE.** owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.RJE.** owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')

pe JES2.** cl(writer) id(<syspau>)
pe JES2.LOCAL.** cl(writer) id(<syspau>)
pe JES2.LOCAL.OFF*.JT cl(writer) id(<syspau>)
pe JES2.LOCAL.OFF*.ST cl(writer) id(<syspau>)
pe JES2.LOCAL.PRT* cl(writer) id(<syspau>)
pe JES2.LOCAL.PUN* cl(writer) id(<syspau>)
pe JES2.NJE.** cl(writer) id(<syspau>)
pe JES2.RJE.** cl(writer) id(<syspau>)
setr racl(writer) Ref
```

CCI: CCI-000213

Group ID (Vulid): V-6922

Group Title: ZJES0032

Rule ID: SV-74871r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0032](#)

Rule Title: JES2 output devices must be properly controlled for Classified Systems.

Vulnerability Discussion: JES2 output devices provide a variety of channels to which output can be processed. Failure to properly control these output devices could result in unauthorized personnel accessing output. This exposure may compromise the confidentiality of customer data on a classified System..

Responsibility: N/A

IAControls: N/A

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- Classification of System
- SENSITIVE.RPT(WRITER)

If the Classification of the system is unclassified, this is not applicable.

Verify that the accesses for WRITER resources are restricted. If the following guidance is true, this is not a finding.

___ The ACF2 resources and/or generic equivalent are defined with a default access of PREVENT.

___ The ACF2 resources and/or generic equivalent identified below will be defined with access restricted to the operators and system programming personnel:

JES2.LOCAL.devicename

JES2.LOCAL.OFFn.*

JES2.LOCAL.OFFn.JT

JES2.LOCAL.OFFn.ST

JES2.LOCAL.PRTn

JES2.LOCAL.PUNn

JES2.NJE.nodename

JES2.RJE.devicename

NOTE: Common sense should prevail during the analysis. For example, access to the offload output destinations should be limited to only systems personnel (e.g., operations staff/system programmers) on a classified system.

Fix Text: Verify with the ISSO to see that access authorization for resources defined to the WRITER resource class is restricted to the operators and system programmers on a classified system only.

Define resources in the ACP s respective WRITER class for each of the following output destinations:

JES2.LOCAL.devicename
JES2.LOCAL.OFFn.*
JES2.LOCAL.OFFn.JT
JES2.LOCAL.OFFn.ST
JES2.LOCAL.PRTn
JES2.LOCAL.PUNn
JES2.NJE.nodename
JES2.RJE.devicename

The resource definition will be generic if all of the resources of the same type have identical access controls (e.g., if all off load transmitters are equivalent). If all users are permitted to route output to a specific destination, the resource controlling it may be defined with a default access of either NONE or READ. Otherwise it will be defined with a default access of NONE.

CCI: CCI-000213

Group ID (Vulid): V-6923

Group Title: ZJES0041

Rule ID: SV-7332r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0041](#)

Rule Title: JESSPOOL resources are not protected in accordance with security requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG, JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing userid and password information. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

JESSPOOL Resource Controls

a) Refer to the following reports produced by the ACF2 Data Collection:

- SENSITIVE.RPT(JESSPOOL)
- ACF2CMDS.RPT(RESOURCE) Alternate report
- ACF2CMDS.RPT(ACFGSO)

b) Review the ACFGSO report. If CLASMAP defines JESSPOOL as TYPE(SPL), there is NO FINDING.

NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Refer to the following report produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

c) Ensure the following items are in effect:

1) The CLASMAP record defines the JESSPOOL resource class.

2) The following resources are defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of PREVENT:

```
localnodeid.-  
localnodeid.JES2.$TRCLOG.taskid.-.JESTRACE  
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG
```

NOTE 1: These resource rules may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

```
localnodeid.JES2.-.-.JESTRACE  
localnodeid.+MASTER+.-.-.
```

NOTE 2: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid.

3) The following resource is defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of READ:

```
localnodeid.jesid.$JESNEWS.taskid.Dnews1v1.JESNEWS
```

jesid The logonid associated with your JES2 system.

NOTE: This resource rule may be more generic as long as it pertains directly to the JESNEWS data set. For example:

localnodeid.jesid.\$JESNEWS.-.-JESNEWS

d) If all of the items in (b) and (c) are true, there is NO FINDING.

e) If any item in (b) or (c) is untrue, this is a FINDING.

Fix Text: Ensure that the CLASMAP defines JESSPOOL as TYPE(SPL).

NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Ensure the following items are in effect:

The CLASMAP record defines the JESSPOOL resource class.

Example:

SHOW CLASMAP

The following resources are defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of PREVENT:

localnodeid.-
localnodeid.JES2.\$TRCLOG.taskid.-.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG

Example:

\$KEY(localnodeid) TYPE(SPL)
- UID(*) PREVENT

NOTE 1: These resource rules may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

localnodeid.JES2.-.-.JESTRACE
localnodeid.+MASTER+.-.-.-

NOTE 2: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid.

The following resource is defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of READ:

localnodeid.jesid.\$JESNEWS.taskid.Dnews1v1.JESNEWS

jesid The logonid associated with your JES2 system.

NOTE: This resource rule may be more generic as long as it pertains directly to the JESNEWS data set. For example:

localnodeid.jesid.\$JESNEWS.-.-.JESNEWS

CCI: CCI-000213

Group ID (Vulid): V-6924

Group Title: ZJES0042

Rule ID: SV-7329r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0042](#)

Rule Title: JESNEWS rewsources are not protected in accordance with security requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG, JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing userid and password information. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

JESSPOOL Resource Controls

a) Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(OPERCMDS)
- ACF2CMDS.RPT(RESOURCE) Alternate report

NOTE: Review the ACFGSO report. If CLASMAP defines OPERCMDS as anything other than TYPE(OPR), replace OPR below with the appropriate three letters.

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(SUBSYS)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZJES0042)

b) Review the resource rules for the OPERCMDS resource class (i.e., TYPE(OPR)) and ensure the following items are in effect:

1) The JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource class with a default access of PREVENT.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

2) Access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts DELETE service to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.

c) If both of the items in (b) are true, there is NO FINDING.

d) If either item in (b) is untrue, this is a FINDING.

Fix Text: JESNEWS Access Controls

Refer to "Protecting JESNEWS" in Chapter 7 of the JES2 Init & Tuning Guide.

a) Ensure the following items are in effect:

1) The JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource class with a default access of NONE and all access is logged.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

2) Access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.

Examples of setting up proper protection are shown here:

```
RDEF OPERCMDS JES2.UPDATE.JESNEWS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('COMPLY WITH ZJES0042')
```

```
PERMIT JES2.UPDATE.JESNEWS CLASS(OPERCMDS) ID(<syspaut>) ACCESS(CONTROL)
```

CCI: CCI-000213

CCI: CCI-001762

CCI: CCI-002234

Group ID (Vulid): V-6925

Group Title: ZJES0044

Rule ID: SV-7334r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0044](#)

Rule Title: JESTRACE and/or SYSLOG resources are not protected in accordance with security requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG, JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing userid and password information. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(JESSPOOL)
- ACF2CMDS.RPT(RESOURCE) Alternate report
- ACF2CMDS.RPT(ACFGSO)

- ACF2CMDS.RPT(LOGONIDS)

NOTE: Review the ACFGSO report. If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Refer to the following report produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

Review the following resources in the JESSPOOL resource class (i.e., TYPE(SPL)):

localnodeid.JES2.\$TRCLOG.taskid.-.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG or
localnodeid.+BYPASS+.SYSLOG.jobid.-.SYSLOG

NOTE: These resource rules may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

localnodeid.JES2.-.-.JESTRACE
localnodeid.+MASTER+.-.-.SYSLOG or
localnodeid.+BYPASS+.-.-.SYSLOG

NOTE: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid. Another method is to issue the JES2 command \$D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

Ensure that access authorization for the resources mentioned above is restricted to the following:

- 1) Logonid(s) associated with external writer(s) can have complete access.

NOTE: An external writer is an STC that removes data sets from the JES spool. In this case, it is responsible for archiving the JESTRACE and SYSLOG data sets. The STC default name is XWTR and the external writer program is called IASXWR00.

- 2) Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems can have complete access.
- 3) Application Development and Application Support personnel responsible for diagnosing application problems can have READ access to the SYSLOG resource.

Fix Text: The IAO will ensure that access authorization for resources defined to the JESTRACE and SYSLOG resources in the JESSPOOL resource class is restricted to the appropriate personnel.

Review the following resources defined to the JESSPOOL resource class:

Ensure the following resources are defined to the JESSPOOL resource class with a UACC(NONE):

```
localnodeid.JES2.$TRCLOG.taskid.*.JESTRACE  
localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG or  
localnodeid.+BYPASS+.SYSLOG.jobid.*.SYSLOG
```

NOTE: These resource profiles may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

```
localnodeid.JES2.$TRCLOG.*.**  
localnodeid.+MASTER+.SYSLOG.*.** or  
localnodeid.+BYPASS+.SYSLOG.*.**
```

NOTE: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid. Another method is to issue the JES2 command \$D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

Ensure that access authorization for the resources mentioned above is restricted to the following:

Userid(s) associated with external writer(s) can have complete access.

NOTE: An external writer is a STC that removes data sets from the JES spool. In this case, it is responsible for archiving the JESTRACE and SYSLOG data sets. The STC default name is XWTR and the external writer program is called IASXWR00.

Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems can have complete access.

Application Development and Application Support personnel responsible for diagnosing application problems can have READ access to the SYSLOG resource.

Examples:

```
RDEFINE JESSPOOL localnodeid.JES2.$TRCLOG.*.** audit(failures(read)) uacc(NONE) -  
data('Reference srr finding ZJES0044 ') owner(admin)
```

```
RDEFINE JESSPOOL localnodeid.+MASTER+.SYSLOG.*.** audit(failures(read)) uacc(NONE) -  
data('Reference srr finding ZJES0044') owner(admin)  
or  
RDEFINE JESSPOOL localnodeid.+BYPASS+.SYSLOG.*.** audit(failures(read)) uacc(NONE) -  
data('Reference srr finding ZJES0044') owner(admin)
```

PE localnodeid.JES2.\$TRCLOG.** cl(jesspool) id(<syspau< <secaudt>) acc(a)
PE localnodeid.+MASTER+.SYSLOG.** cl(jesspool) id(<syspau< <secaudt>) acc(a)
PE localnodeid.+MASTER+.SYSLOG.** cl(jesspool) id(<appdpau< <appsaudt>) acc(r)
or
PE localnodeid.+BYPASS+.SYSLOG.** cl(jesspool) id(<syspau< <secaudt>) acc(a)
PE localnodeid.+BYPASS+.SYSLOG.** cl(jesspool) id(<appdpau< <appsaudt>) acc(r)

CCI: CCI-000213

CCI: CCI-001762

Group ID (Vulid): V-6926

Group Title: ZJES0046

Rule ID: SV-7336r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0046](#)

Rule Title: JES2 spool resources will be controlled in accordance with security requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG, JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing userid and password information. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(JESSPOOL)
- ACF2CMDS.RPT(RESOURCE) Alternate report
- ACF2CMDS.RPT(ACFGSO)

Verify that the accesses to the JESSPOOL resources are properly restricted. If the following guidance is true, this is not a finding.

Review the ACFGSO report, a CLASMAP will define JESSPOOL as TYPE(SPL).

NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Review the JESSPOOL report for resource rules with the following naming convention. These rules may be fully qualified, be specified as generic, or be specified with masking as indicated below:

localnodeid.logonid.jobname.jobid.dsnumber.name

| | |
|-------------|---|
| localnodeid | The name of the node on which the SYSIN or SYSOUT data set currently resides. |
| Logonids | The logonid associated with the job. This is the logonid ACF2 uses for validation purposes when the job runs. |
| jobname | The name that appears in the name field of the JOB statement. |
| jobid | The job number JES2 assigned to the job. |
| dsnumber | The unique data set number JES2 assigned to the spool data set. A D is the first character of this qualifier. |
| name | The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify DSN= on the DD statement that creates the spool data set, JES2 uses a question mark (?). |

All users have access to their own JESSPOOL resources.

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel, with access to allow all SERVICES or any combination of SERVICE(). All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.-.-, localnodeid.-, etc)

The JESSPOOL localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked, can be made available to users, when approved by the IAO. Access will be identified at the minimum access for the user to accomplish the users function, SERVICE(READ, UPDATE, DELETE, ADD). All access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes.

CSSMTP will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the IAO. All access will be logged.

Spooling products users (CA-SPOOL, CA View, etc.) will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the IAO. Logging of access is not required.

Fix Text: The IAO will develop a plan of action to implement the required changes. Ensure the following items are in effect for JESSPOOL resources. The JESSPOOL may have more restrictive security at the direction of the IAO.

The JESSPOOL resources may be fully qualified, be specified as generic, or be specified with masking as indicated below:

localnodeid.userid.jobname.jobid.dsnumber.name

| | |
|-------------|---|
| localnodeid | The name of the node on which the SYSIN or SYSOUT data set currently resides. |
|-------------|---|

| | |
|--------|--|
| userid | The userid associated with the job. This is the userid used for validation purposes when the job runs. |
|--------|--|

jobname The name that appears in the name field of the JOB statement.

jobid The job number JES2 assigned to the job.

dsnumber The unique data set number JES2 assigned to the spool data set. A D is the first character of this qualifier.

name The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify DSN= on the DD statement that creates the spool data set, JES2 uses a question mark (?).

By default a user has access only to that user's own JESSPOOL resources. However, situations exist where a user legitimately requires access to jobs that run under another user's userid. In particular, if a user routes SYSOUT to an external writer, the external writer should have access to that user's SYSOUT.

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel with access of ALTER. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc)

```
RDEF JESSPOOL localnodeid.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('PROTECT JESSPOOL AT HIGH LEVEL, REF
ZJES0046')
PE localnodeid.** CL(JESSPOOL) ID(syspautd) ACC(A)
```

The JESSPOOL localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked, can be made available to users, when approved by the IAO. Access will be identified at the minimum access for the user to accomplish the user's function, SERVICE(READ, UPDATE, DELETE, ADD). All access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes. If frequent situations occur where users working on a common project require selective access to each other's jobs, then the installation may delegate to the individual users the authority to grant access, but only with the approval of the IAO.

```
RDEF JESSPOOL localnode.userid.jobname.jobid.dsnumber.name
UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('PROTECT JESSPOOL, REF ZJES0046')
PE localnode.userid.jobname.jobid.dsnumber.name CL(JESSPOOL) ID(<users_or_groups>) ACC(R)
```

If IBM's SDSF product is installed on the system, resources defined to the JESSPOOL resource class control functions related to jobs, output groups, and SYSIN/SYSOUT data sets on various SDSF panels.

CSSMTP will not be granted to the JESSPOOL resource of the high level node. or localnodeid. . CSSMTP can have access to the specific approved JESSPOOL resources, minimally qualified to the node.userid. and all access will be logged. This will ensure system records who (userid) sent traffic to CSSMTP, when and what job/process.

Spooling products users (CA-SPOOL, CA View, etc.) will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the IAO. Logging of access is not required.

The IAO will review JESSPOOL resource rules. If a rule has been determined not to have been used within the last 2 years, the rule shall be removed.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6927

Group Title: ZJES0051

Rule ID: SV-00000r0_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0051](#)

Rule Title: JES2.** resource is not protected in accordance with security requirements.

Vulnerability Discussion: JES2 system commands are used to control JES2 resources and the operating system environment. Failure to properly control access to JES2 system commands could result in unauthorized personnel issuing sensitive JES2 commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: CCI-000213

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(OPERCMDS)
- ACF2CMDS.RPT(RESOURCE) Alternate report
- ACF2CMDS.RPT(ACFGSO)

NOTE: Review the ACFGSO report. If CLASMAP defines OPERCMDS as anything other than TYPE(OPR), replace OPR below with the appropriate three letters.

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(SUBSYS)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZJES0051)
- b) Review resource rules for TYPE(OPR).
- c) If the JES2.- resource is defined to the OPERCMDS class, there is NO FINDING.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

- d) If the JES2.- resource is NOT defined to the OPERCMDS class, this is a FINDING.

Fix Text:

The IAO will ensure that the JES2.* resource is defined to the OPERCMDS class with a default of no access and all access is logged.

If CLASMAP defines OPERCMDS as anything other than TYPE(OPR), replace OPR below with the appropriate three letters.

Review resource rules for TYPE(OPR).

Ensure the JES2.- resource is defined to the OPERCMDS class.

Example:

SHOW CLASMAP

\$KEY(JES2) TYPE(OPR)
- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-6928

Group Title: ZJES0052

Rule ID: SV-17410r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0052](#)

Rule Title: JES2 system commands are not protected in accordance with security requirements.

Vulnerability Discussion: JES2 system commands are used to control JES2 resources and the operating system environment. Failure to properly control access to JES2 system commands could result in unauthorized personnel issuing sensitive JES2 commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(OPERCMDS)
- ACF2CMD5.RPT(RESOURCE) Alternate report
- ACF2CMD5.RPT(ACFGSO)
- ACF2CMD5.RPT(LOGONIDS)

NOTE: Review the ACFGSO report. If CLASMAP defines OPERCMD5 as anything other than TYPE(OPR), replace OPR below with the appropriate three letters.

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZJES0052)

b) Review resource rules for TYPE(OPR).

c) If the JES2.- resource is defined to the OPERCMD5 class with a default access of PREVENT and all access is logged, there is NO FINDING.

d) If access to JES2 system commands defined in the table entitled Controls on JES2 System Commands, in the z/OS STIG Addendum is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), there is NO FINDING.

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

e) If access to specific JES2 system commands is logged as indicated in the table entitled Controls on JES2 System Commands, in the z/OS STIG Addendum, there is NO FINDING.

f) If either (c), (d), or (e) above is untrue for any JES2 system command resource, this is a FINDING.

Fix Text: Extended MCS support allows the installation to control the use of JES2 system commands through the ACP. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

To control access to JES2 system commands, apply the following recommendations when implementing security:

- 1) Define the JES2.** resource in the OPERCMDS class with a default access of NONE and all access is logged.
- 2) Define the JES2 system commands as specified in the "Controls on JES2 System Commands" table, in the zOS STIG Addendum restricts access to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

- 3) Define the JES2 system commands with proper logging as specified in the "Controls on JES2 System Commands" table, in the zOS STIG Addendum.

Build a command file based on the referenced JES2 Command Table. A sample of the commands in the command file is provided here:

```
RDEF OPERCMDS JES2.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED BY SRR PDI ZJES0052')
```

```
RDEF OPERCMDS JES2.<command>.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED BY SRR PDI ZJES0052')  
PE JES2.<command>.** CL(OPERCMDS) ID(<syspautd>) ACC(U)
```

```
SETR RACL(OPERCMDS) REF
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-54

Group Title: ZJES0060

Rule ID: SV-7346r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ZJES0060](#)

Rule Title: Surrogate users must be controlled in accordance with proper security requirements.

Vulnerability Discussion: Surrogate users have the ability to submit jobs on behalf of another user (the execution user) without specifying the execution user's password. Jobs submitted by surrogate users run with the identity of the execution user. Failure to properly control surrogate users could result in unauthorized personnel accessing sensitive resources. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following reports produced by the ACF2 Data Collection:

- SENSITVE.RPT(SURROGAT)
- ACF2CMDS.RPT(RESOURCE) Alternate report
- ACF2CMDS.RPT(ACFGSO)

Review the ACFGSO report executionuserid.SUBMIT resources. These are usually defined to CLASMAP as TYPE(SUR).

NOTE: If CLASMAP defines SURROGAT as anything other than TYPE(SUR), replace SUR below with the appropriate three letters.

If no executionuserid.SUBMIT resources are defined to the SURROGAT resource class, this is not applicable.

If executionuserid.SUBMIT resources are defined to the SURROGAT resource class, review resource rules for TYPE(SUR) if the following items are in effect, this is not a finding.

___ All executionlogonid.SUBMIT resources defined to the SURROGAT class specify a default access of PREVENT.

___ All resource access is logged; at the discretion of the ISSM/ISSO scheduling tasks may be exempted.

___ Access authorization is restricted to scheduling tools, started tasks or other system applications required for running production jobs.

___ Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent).

Fix Text: For executionuserid.SUBMIT resources defined to the SURROGAT resource class, ensure the following items are in effect regarding surrogate controls:

All executionuserid.SUBMIT resources defined to the SURROGAT resource class specify a default access of NONE.

All resource access is logged except for scheduling tasks. This is optional and the ISSM/ISSO scheduling tasks may be exempted. Access authorization is restricted to scheduling tools, started tasks or other system applications required for running production jobs.

Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent).

Consider the following recommendations when implementing security for Surrogate Users:

Keep the use of Surrogate Users outside of those granted to the scheduling software to a minimum number of individuals. The simplest configuration is to only use Surrogate resource for the appropriate Scheduling task/software for production scheduling purposes as documented.

Temporary use of surrogate resource of the production batch to the scheduling tasks may be allowed for a period for testing by the appropriate specific production Support Team members. Authorization, eligibility and test period is determined by site policy.

Access authorization is restricted to the minimum number of personnel required for running production jobs. However, Surrogate usage should not become the default for all jobs submitted by individual userids (i.e., system programmer shall use their assigned individual userids for software installation, duties, whereas a Cross Authorized ACID would normally be utilized for scheduled batch production only and as such shall normally be limited to the scheduling task such as CONTROLM) and not granted as a normal daily basis to individual users..

Command samples are provided to define/permit SURROGAT profiles:

```
SETR CLASSACT(SURROGAT)
SETR GENERIC(SURROGAT) GENCMD(SURROGAT)
SETR RACL(SURROGAT)
```

```
RDEF SURROGAT <batchid>..SUBMIT UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('SUBMIT JOBS FOR <batchid>, REFERENCE
ZJES0060')
```

```
PE <batchid>..SUBMIT CL(SURROGAT) ID(<authorized user such as CONTROLM>)
```

CCI: CCI-000213

CCI: CCI-002233

CCI: CCI-002234

Group ID (Vulid): V-31

Group Title: ZSMS0010

Rule ID: SV-7355r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSMS0010](#)

Rule Title: DFSMS resources must be protected in accordance with the proper security requirements.

Vulnerability Discussion: DFSMS provides data, storage, program, and device management functions for the operating system. Some DFSMS storage administration functions allow a user to obtain a privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ZSMS0010)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZSMS0010)

Ensure that all SMS resources and/or generic equivalent are properly protected according to the requirements specified. If the following guidance is true, this is not a finding.

___ The resource rule for FACILITY (FAC) \$KEY(STGADMIN) has a default access of PREVENT.

___ STGADMIN.DPDSRN.olddname is restricted to System Programmers and all access is logged.

___ The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to System Programmers and all access is logged.

___ The STGADMIN.IGG.DEFDEL.UALIAS is restricted to Centralized and Decentralized Security personnel and System Programmers and all access is logged.

To avoid authorization failures once a base cluster is accessed via a PATH or AIX by a user or application that has authority to the PATH and AIX, but not the base cluster, APAR OA50118 must be applied.

The resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE is defined with access of PREVENT
The resource STGADMIN.IGG.CATALOG.SECURITY.BOTH is defined with access of READ

Note: the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE can be defined with read access for migration purposes. If it is, a detailed migration plan must be documented and filed by the ISSM that determines a definite migration period. All access must be logged. At the completion of migration this resource must be configured with access = PREVENT.

If the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE and STGADMIN.IGG.CATALOG.SECURITY.BOTH are both defined, STGADMIN.IGG.CATALOG.SECURITY.BOTH takes precedence.

___ The following resources and prefixes may be available to the end-user.

STGADMIN.ADR.COPY.CNCURRNT
STGADMIN.ADR.COPY.FLASHCPY
STGADMIN.ADR.COPY.TOLERATE.ENQF
STGADMIN.ADR.DUMP.CNCURRNT
STGADMIN.ADR.DUMP.TOLERATE.ENQF
STGADMIN.ADR.RESTORE.TOLERATE.ENQF
STGADMIN.ARC.ENDUSER.
STGADMIN.IGG.ALTER.SMS

___ The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and System programmers.

STGADMIN.IDC.DCOLLECT

___ The following resources are restricted to Application Production Support Team members, DASD managers, and System programmers.

STGADMIN.ARC.CANCEL
STGADMIN.ARC.LIST
STGADMIN.ARC.QUERY
STGADMIN.ARC.REPORT
STGADMIN.DMO.CONFIG
STGADMIN.IFG.READVTOC
STGADMIN.IGG.DELGDG.FORCE

___ The following resource prefixes, at a minimum, are restricted to DASD managers and System programmers.

STGADMIN.ADR
STGADMIN.ANT
STGADMIN.ARC
STGADMIN.DMO
STGADMIN.ICK
STGADMIN.IDC
STGADMIN.IFG
STGADMIN.IGG
STGADMIN.IGWSHCDS

___ The following Storage Administrator functions prefix is restricted to DASD managers and System programmers and all access is logged.

STGADMIN.ADR.STGADMIN.

Fix Text: Ensure that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Below is listed the access requirements for SMS Resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent are followed.

The ACF2 resources are defined with a default access of PREVENT.

Ensure that the following items are in effect:

Ensure that no access is given to the high-level STGADMIN resource.

Example:

\$KEY(STGADMIN) TYPE(FAC)

- UID(*) PREVENT

To avoid authorization failures once a base cluster is accessed via a PATH or AIX by a user or application that has authority to the PATH and AIX, but not the base cluster, APAR OA50118 must be applied.

Configure resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE with no access .

Example:

\$KEY(STGADMIN) TYPE(FAC)

IGG.STGADMIN.IGG.CATALOG.SECURITY.CHANGE-UID(*) PREVENT

Configure resource IGG.STGADMIN.IGG.CATALOG.SECURITY.BOTH with READ access for all.

\$KEY(STGADMIN) TYPE(FAC)

IGG.STGADMIN.IGG.CATALOG.SECURITY.BOTH-UID(*) READ

Note: the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE can be defined with read access for migration purposes. If it is a detailed migration plan must be documented and filed with the ISSM that determines a definite migration period. All access must be logged. At the completion of migration this resource must be configured with access = PREVENT

If the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE and STGADMIN.IGG.CATALOG.SECURITY.BOTH are both defined, STGADMIN.IGG.CATALOG.SECURITY.BOTH takes precedence.

The STGADMIN.DPDSRN.olddsrname is restricted to System Programmers and all access is logged.

Example:

\$KEY(STGADMIN) TYPE(FAC)

DPDSRN.- UID(syspau dt) SERVICE(READ) LOG

DPDSRN.- UID(*) PREVENT

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to System Programmers and all access is logged.

Example:

\$KEY(STGADMIN) TYPE(FAC)

IGD.ACTIVATE.CONFIGURATION UID(syspau dt) SERVICE(READ) LOG

IGD.ACTIVATE.CONFIGURATION UID(*) PREVENT

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to System Programmers and Security personnel and all access is logged.

Example:

\$KEY(STGADMIN) TYPE(FAC)

IGG.DEFDEL.UALIAS UID(secau dt) SERVICE(READ) LOG

IGG.DEFDEL.UALIAS UID(secdau dt) SERVICE(READ) LOG

IGG.DEFDEL.UALIAS UID(syspau dt) SERVICE(READ) LOG

IGG.DEFDEL.UALIAS UID(*) PREVENT

The following resources and prefixes may be available to the end-user.

STGADMIN.ADR.COPY.CNCURRNT

STGADMIN.ADR.COPY.FLASHCPY
STGADMIN.ADR.COPY.TOLERATE.ENQF
STGADMIN.ADR.DUMP.CNCURRNT
STGADMIN.ADR.DUMP.TOLERATE.ENQF
STGADMIN.ADR.RESTORE.TOLERATE.ENQF
STGADMIN.ARC.ENDUSER.
STGADMIN.IGG.ALTER.SMS

Example:

\$KEY(STGADMIN) TYPE(FAC)
ADR.COPY.CNCURRNT.- UID(endusers) SERVICE(READ)

The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and System programmers.

STGADMIN.IDC.DCOLLECT

Example:

\$KEY(STGADMIN) TYPE(FAC)
IDC.DCOLLECT.- UID(appsaudt) SERVICE(READ)
IDC.DCOLLECT.- UID(autoaudt) SERVICE(READ)
IDC.DCOLLECT.- UID(dasbaudt) SERVICE(READ)
IDC.DCOLLECT.- UID(dasdaudt) SERVICE(READ)
IDC.DCOLLECT.- UID(syspaudt) SERVICE(READ)
IDC.DCOLLECT.- UID(*) PREVENT

The following resources are restricted to Application Production Support Team members, DASD managers, and System programmers.

STGADMIN.ARC.CANCEL
STGADMIN.ARC.LIST
STGADMIN.ARC.QUERY
STGADMIN.ARC.REPORT
STGADMIN.DMO.CONFIG
STGADMIN.IFG.READVTOC
STGADMIN.IGG.DELGDG.FORCE

Example:

\$KEY(STGADMIN) TYPE(FAC)

ARC.CANCEL.- UID(appsaudt) SERVICE(READ)
ARC.CANCEL.- UID(dasbaudt) SERVICE(READ)
ARC.CANCEL.- UID(dasdaudt) SERVICE(READ)
ARC.CANCEL.- UID(syspauDt) SERVICE(READ)
ARC.CANCEL.- UID(*) PREVENT

The following resource prefixes, at a minimum, are restricted to DASD managers and System programmers.

STGADMIN.ADR
STGADMIN.ANT
STGADMIN.ARC
STGADMIN.DMO
STGADMIN.ICK
STGADMIN.IDC
STGADMIN.IFG
STGADMIN.IGG
STGADMIN.IGWSHCDS

Example:

\$KEY(STGADMIN) TYPE(FAC)
ADR. - UID(dasbaudt) SERVICE(READ)
ADR.- UID(dasdaudt) SERVICE(READ)
ADR.- UID(syspauDt) SERVICE(READ)
ADR.- UID(*) PREVENT

The following Storage Administrator functions prefix is restricted to DASD managers and System programmers and all access is logged.

STGADMIN.ADR.STGADMIN.

Example:

\$KEY(STGADMIN) TYPE(FAC)
ADR.STGADMIN.- UID(dasbaudt) SERVICE(READ) LOG
ADR.STGADMIN.- UID(dasdaudt) SERVICE(READ) LOG
ADR.STGADMIN.- UID(syspauDt) SERVICE(READ) LOG
ADR.STGADMIN.- UID(*) PREVENT

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6933

Group Title: ZSMS0012

Rule ID: SV-7350r4_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSMS0012](#)

Rule Title: SMS Program Resources must be properly defined and protected.

Vulnerability Discussion: DFSMS provides data, storage, program, and device management functions for the operating system. Some DFSMS storage administration functions allow a user to obtain a privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data.

Responsibility: Systems Programmer

IAControls: N/A

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ZSMS0012)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZSMS0012)

Ensure that all SMS Program resources and/or generic equivalent are properly protected according to the requirements specified in SMS Program Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

___ The ACF2 resources are defined with a default access of PREVENT.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Use SMS Program Resources table in the z/OS STIG Addendum. This table lists the resources, access requirements for SMS Program Resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent specified in the z/OS STIG Addendum are followed.

The ACF2 resources as designated in the above table are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The following commands are provided as a sample for implementing resource controls:

```
$KEY(ACBFUTO2) TYPE(PGM)
UID(audtaudt) ALLOW
UID(dasdaudt) ALLOW
UID(secaudt) ALLOW
UID(syspauudt) ALLOW
UID(tstcaudt) ALLOW
UID(*) PREVENT
```

```
F ACF2,REBUILD(PGM)
```

CCI: CCI-000213

Group ID (Vulid): V-3895

Group Title: ZSMS0020

Rule ID: SV-7357r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSMS0020](#)

Rule Title: DFSMS control data sets are not protected in accordance with security requirements.

Vulnerability Discussion: DFSMS control data sets provide the configuration and operational characteristics of the system-managed storage environment. Failure to properly protect these data sets may result in unauthorized access. This exposure could compromise the availability and integrity of some system services and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(SMSRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZSMS0020)

b) Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)

Active Control Data Set (ACDS)

Communications Data Set (COMMDS)

Automatic Class Selection Routine Source Data Sets (ACS)

ACDS Backup

COMMDS Backup

c) If the ACF2 data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALLOCATE access to only systems programming personnel, this not is a finding

d) If the ACF2 data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict UPDATE and ALLOCATE access to only systems programming personnel, this is a finding.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control datasets.

Fix Text: Ensure that DFSMS control data sets restrict UPDATE or ALLOCATE access to system programmers responsible for DASD management. Justification is required for any additional access.

Review the SYS1.PARMLIB(IGDSMSxx) data set to identify the fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)

Active Control Data Set (ACDS)

Communications Data Set (COMMDS)

Automatic Class Selection Routine Source Data Sets (ACS)

ACDS Backup

COMMDS Backup

Ensure the ACF2 data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALLOCATE access to only systems programming personnel.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control datasets.

Example:

```
$KEY(S3D)
$PREFIX(SYS3)
DFSMS.MVA.ACDS UID(syspautd) R(A) W(L) A(L) E(A)
DFSMS.MVA.COMMDS UID(syspautd) R(A) W(L) A(L) E(A)
DFSMS.MVA.SCDS UID(syspautd) R(A) W(L) A(L) E(A)
DFSMS.MVA.ACS UID(syspautd) R(A) W(L) A(L) E(A)
```

CCI: CCI-000213

Group ID (Vulid): V-6936

Group Title: ZSMS0022

Rule ID: SV-7237r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSMS0022](#)

Rule Title: DFSMS control data sets are not properly protected.

Vulnerability Discussion: DFSMS control data sets provide the configuration and operational characteristics of the system-managed storage environment. Failure to properly protect these data sets may result in unauthorized access. This exposure could compromise the availability and integrity of some system services and customer data.

Responsibility: Information Assurance Officer

IAControls: COTR-1, DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

Active Control Data Set (ACDS)

Communications Data Set (COMMDS)

Refer to the report produced in previous PDI(ZSMSR020) for the data set volume serial number:

Refer to the following item gathered from the Data Facility Storage Management Subsystem (DFSMS) Worksheet in the Preliminary Information Worksheets in U_zOS_STIG_INSTRUCTION.doc:

___ 1. Provide the following DFSMS data set names:

SCDS:

ACDS:

COMMDS:

ACS:

ACDS Backup:

COMMDS Backup:

b) If the COMMDS and ACDS SMS data sets identified in (a) above reside on different volumes, there is NO FINDING.

c) If the COMMDS and ACDS SMS data sets identified in (a) above are collocated on the same volume, this is a FINDING.

Fix Text: The systems programmer will see that the primary and backup SMS Control data sets are allocated on separate volumes.

- (a) Source Control Data Set (SCDS) contains a SMS configuration, which defines a storage management policy.
 - (b) Active Control Data Set (ACDS) contains a copy of the most recently activated configuration. All systems in a SMS complex use this configuration to manage storage.
 - (c) Communications Data Set (COMMDS) contains the name of the ACDS containing the currently active storage management policy, the current utilization statistics for each system managed volume, and other system information.
- (2) The ACDS data set will reside on a different volume than the COMMDS data set.

Allocate backup copies of the ADCS and COMMD5 data sets on a different shared volume from the primary ACDS and COMMD5 data sets.

CCI: CCI-000549

Group ID (Vulid): V-3896

Group Title: ZSMS0030

Rule ID: SV-3896r2_rule

Severity: CAT III

Rule Version (STIG-ID): [ZSMS0030](#)

Rule Title: SYS(x).Parmlib(IEFSSNxx) SMS configuration parameter settings are not properly specified.

Vulnerability Discussion: Configuration properties of DFSMS are specified in various members of the system parmlib concatenation (e.g., SYS1.PARMLIB). Statements within these PDS members provide the execution, operational, and configuration characteristics of the system-managed storage environment. Missing or inappropriate configuration values may result in undesirable operations and degraded security. This exposure could potentially compromise the availability and integrity of some system services and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Review the logical parmlib data sets, example: SYS1.PARMLIB(IEFSSNxx), for one of the following SMS parameter settings:

1. Keyword syntax:

SUBSYS SUBNAME(SMS) INITRTN(IGDSSIIN)

2. Positional syntax:

SMS, IGDSSIIN

b) If the required parameters are defined, there is NO FINDING.

c) If the required parameters are not defined, this is a FINDING.

Fix Text: Review the DFSMS-related PDS members and statements specified in the system parmlib concatenation. Ensure these elements are configured as outlined below

Keyword syntax:

SUBSYS SUBNAME(SMS) INITRTN(IGDSSIIN)

Positional syntax:

SMS, IGDSSIIN

CCI: CCI-000366

Group ID (Vulid): V-6937

Group Title: ZSMS0032

Rule ID: SV-7238r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSMS0032](#)

Rule Title: SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings are not properly specified.

Vulnerability Discussion: Configuration properties of DFSMS are specified in various members of the system parmlib concatenation (e.g., SYS1.PARMLIB). Statements within these PDS members provide the execution, operational, and configuration characteristics of the system-managed storage environment. Missing or inappropriate configuration values may result in undesirable operations and degraded security. This exposure could potentially compromise the availability and integrity of some system services and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), for the following SMS parameter settings:

Parameter Key
SMS

ACDS(ACDS data set name)
COMMDS(COMMDS data set name)

- b) If the required parameters are defined, there is NO FINDING.
- c) If the required parameters are not defined, this is a FINDING.

Fix Text: The Systems programmer will review the DFSMS-related PDS members and statements specified in the system parmlib concatenation. Ensure these elements are configured as outlined below:

Parameter Key
SMS
ACDS(ACDS data set name)
COMMDS(COMMDS data set name)

CCI: CCI-000366

Group ID (Vulid): V-6943

Group Title: ZSMSA008

Rule ID: SV-7244r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSMSA008](#)

Rule Title: DFSMS resource class(es) is(are) not defined to the GSO CLASMAP record in accordance with security requirements.

Vulnerability Discussion: DFSMS provides data, storage, program, and device management functions for the operating system. Some DFSMS storage administration functions allow a user to obtain a privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

- a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection:

- PDI(ZSMSA008)

- b) Review the GSO CLASMAP record for the following definitions:

MGMTCLAS
STORCLAS

- c) If both resource classes in (b) above are defined, there is NO FINDING.

- d) If either resource class in (b) above is not defined, this is a FINDING.

Fix Text: The IAO will ensure that the MGMTCLAS and STORCLAS resource classes are defined to the GSO CLASSMAP record.

Review the GSO CLASMAP record for the following definitions:

MGMTCLAS
STORCLAS

Ensure both resource classes above are defined.

Example:

SHOW CLASMAP

CCI: CCI-000213

Group ID (Vulid): V-69229

Group Title: ZSSH0010

Rule ID: SV-83851r1_rule

Severity: CAT I

Rule Version (STIG-ID): [ZSSH0010](#)

Rule Title: The SSH daemon must be configured to only use the SSHv2 protocol.

Vulnerability Discussion: SSHv1 is not a DoD-approved protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Responsibility: N/A

IAControls: N/A

Check Content:

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) If SSH Daemon is not active, there is NOFINDING.
- d) Examine SSH daemon configuration file.
 - 1. If variable 'Protocol 2' is defined, there is NO FINDING.
 - 2. If variable 'Protocol' is defined in a leading comment or has a value other than 2, this is a FINDING.

Fix Text: Edit the sshd_config file and set the "Protocol" setting to "2". _____

Group ID (Vulid): V-69231

Group Title: ZSSH0020

Rule ID: SV-83853r1_rule

Severity: CAT I

Rule Version (STIG-ID): [ZSSH0020](#)

Rule Title: The SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm.

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. Cryptographic modules must adhere to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Responsibility: N/A

IAControls: N/A

Check Content:

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.

- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) Examine SSH daemon configuration file sshd_config.
 - 1. If there are no Ciphers lines or the ciphers list contains any cipher not starting with 3des or aes, this is a FINDING.
 - 2. If the Macs line is not configured to hmac-shal or greater, this is a FINDING.
- d) Examine the z/OS-specified sshd server system-wide configuration zos_sshd_config.
 - 1. If any of the following is untrue, this is a FINDING.
 - i. FIPSMODE YES
 - ii. CiphersSource ICSF
 - iii. MACsSource ICSF

Fix Text: Edit the SSH daemon configuration and remove any ciphers not starting with "3des" or "aes". If necessary, add a "Ciphers" line using FIPS 140-2 compliant algorithms.

Configure for message authentication to MACs "hmac-sha1" or greater.

Edit the z/OS-specific sshd server system-wide configuration file configuration as follows:

```
FIPSMODE    YES
CiphersSource    ICSF
MACsSource    ICSF
```

Group ID (Vulid): V-69233

Group Title: ZSSH0030

Rule ID: SV-83855r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSSH0030](#)

Rule Title: The SSH daemon must be configured with the Department of Defense (DoD) logon banner.

Vulnerability Discussion: Failure to display the DoD logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Responsibility: N/A

IAControls: N/A

Check Content:

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
 - b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
 - c) If SSH Daemon is not active, there is NO FINDING.
 - d) Examine SSH daemon configuration file.
- 1. If Banner statement is missing or configured to none, this is a FINDING.
 - 2. Ensure that the contents of the file specified on the banner statement contain a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. If there is any deviation, this is a FINDING.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix Text: Configure the banner statement to a file that contains the Department of Defense (DoD) logon banner.

Ensure that the contents of the file specified on the banner statement contain a logon banner.

The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Group ID (Vulid): V-69235

Group Title: ZSSH0040

Rule ID: SV-83857r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSSH0040](#)

Rule Title: SMF recording options for the SSH daemon must be configured to write SMF records for all eligible events.

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit trails from each of the ACPs. If the control options for the recording of this tracking are not properly maintained, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Responsibility: N/A

IAControls: N/A

Check Content:

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.

- c) If SSH Daemon is not active, there is NO FINDING.
- d) Examine SSH daemon configuration file.
- 1. If Server SMF is not coded with ServerSMF TYPE119_U83, this is a FINDING.
- 2. If Server SMF is commented out, this is a FINDING

Fix Text: Configure the SERVERSMF statement in the SSH Daemon configuration file to TYPE119_U83.

Group ID (Vulid): V-69237

Group Title: ZSSH0050

Rule ID: SV-83859r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZSSH0050](#)

Rule Title: The SSH daemon must be configured to use SAF keyrings for key storage.

Vulnerability Discussion: The use of SAF Key Rings for key storage enforces organizational access control policies and assures the protection of cryptographic keys in storage.

Responsibility: N/A

IAControls: N/A

Check Content:

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) If SSH Daemon is not active, there is NO FINDING.
- d) Examine SSH daemon configuration file. Ensure the following are either not coded or commented out:

```
#HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
#HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
```

e) Locate the z/OS-specific sshd server system wide configuration file `zos_sshd_config`. This file may be found in the `/etc/ssh/` directory. Ensure that a `HostKeyRingLabel` line is coded and commented out.

f) If either of the above is true, this is a FINDING.

Fix Text: Configure the SSH Daemon configuration file with the following statements

Ensure that the following is either not coded or comment out.

```
#HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
#HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
```

Configure the `zos_sshd_config` with the `HostKeyRingLabel` Statement.

Example:

```
HostKeyRingLabel="SSHDAEM/SSHDring my label"
```

Group ID (Vulid): V-184

Group Title: ZTSO0020

Rule ID: SV-184r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ZTSO0020](#)

Rule Title: LOGONIDs must not be defined to SYS1.UADS for non-emergency use.

Vulnerability Discussion: SYS1.UADS is a dataset where LOGONIDs will be maintained with applicable password information when the ACP is not functional. If an unauthorized user has access to SYS1.UADS, they could enter their LOGONID and password into the SYS1.UADS dataset and could give themselves all special attributes on the system. This could enable the user to bypass all security and alter data. They could modify the audit trail information so no trace of their activity could be found.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) From Analyzer main menu, go to 4;U.

Note: Analyzer 8.1 with PTF VS48081 is required for this option to be

available.

b) Set Exceptions only field to NO. Press <ENTER>.

c) Submit the report.

d) Review the generated report.

e) If SYS1.UADS userids are limited and reserved for emergency purposes only, there is NO FINDING.

f) If any SYS1.UADS userids are assigned for other than emergency purposes, this is a FINDING.

Fix Text: The system programmer and IAO will examine the SYS1.UADS entries to ensure LOGONIDs defined include only those users required to support specific functions related to system recovery. Evaluate the impact of accomplishing the change.

CCI: CCI-000764

Group ID (Vulid): V-297

Group Title: ZTSO0030

Rule ID: SV-297r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZTSO0030](#)

Rule Title: TSOAUTH resources must be restricted to authorized users.

Vulnerability Discussion: The TSOAUTH resource class controls sensitive privileges, such as OPER, ACCOUNT, CONSOLE, and PARMLIB. Several of these privileges offer the ability, or provide a facility, to modify sensitive operating system resources. Failure to properly control and restrict access to these privileges may result in the compromise of the operating system environment, ACP, and customer data.

Potential Impacts:

fix typo error

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(ZTSO0030)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZTSO0030)

Ensure that all TSOAUTH resources and/or generic equivalent are properly protected according to the requirements specified. If the following guidance is true, this is not a finding.

___ The ACCT authorization is restricted to security personnel.

___ The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all user when SDSF is installed at the IAOs discretion.

___ The MOUNT authorization is restricted to DASD batch users only.

___ The OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.).

___ The PARMLIB authorization is restricted to only z/OS systems programming personnel and READ access may be given to auditors.

___ The TESTAUTH authorization is restricted to only z/OS systems programming personnel.

Fix Text: Configure the TSOAUTH resource class to control sensitive TSO/E commands.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Below is listed the access requirements for TSOAUTH resources. Ensure the guidelines for the resources and/or generic equivalent are followed.

The ACCT authorization is restricted to security personnel.

The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all user when SDSF is installed at the IAOs discretion.

The MOUNT authorization is restricted to DASD batch users only.

The OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.).

The PARMLIB authorization is restricted to only z/OS systems programming personnel and READ access may be given to audit users.

The TESTAUTH authorization is restricted to only z/OS systems programming personnel.

CCI: CCI-000213

Group ID (Vulid): V-6944

Group Title: ZUSS0011

Rule ID: SV-7245r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0011](#)

Rule Title: z/OS UNIX OMVS parameters in PARMLIB are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The Systems Programmer will ensure parmlib member IEASYSxx specifies parameter OMVS and does not specify OMVS=DEFAULT.

a) Using Vanguard Analyzer online display select Parmlib Analysis option 3;L. When Parmlib options are displayed press enter to continue. When the Parmlib member list is presented locate the IEASYSxx member and browse this member.

NOTE: If the OMVS statement is not specified, OMVS=DEFAULT is used. This will result (as of Z/OS Release 2.8) in the Z/OS UNIX kernel starting in minimum configuration mode. In minimum mode there is no access to permanent file systems or to the shell, and IBM s Communication Server TCP/IP will not run.

b) If the parameter is specified as OMVS=xx or OMVS=(xx,xx,) in the IEASYSxx member, there is NO FINDING.

c) If the parameter is not specified as OMVS=xx or OMVS=(xx,xx,), this is a FINDING.

Fix Text: Review the settings in PARMLIB and /etc for z/OS UNIX security parameters and ensure that the values conform to the specifications below:

The parameter is specified as OMVS=xx or OMVS=(xx,xx,) in the IEASYSxx member.

NOTE: If the OMVS statement is not specified, OMVS=DEFAULT is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM s Communication Server TCP/IP will not run.

CCI: CCI-000366

Group ID (Vulid): V-6945

Group Title: ZUSS0012

Rule ID: SV-7246r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0012](#)

Rule Title: z/OS UNIX BPXPRMxx security parameters in PARMLIB are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Documentable: YES

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The Systems Programmer will ensure parmlib member BPXPRMxx follows the specifications specified for the above control parameters SUPERUSER, STEPLIBLIST, USERIDALIASTABLE, STARTUP_PROC, and MOUNT.

a) Use Vanguard Analyzer Parmlib Analysis option L. Browse all the BPXPRMxx members.

b) Review the logical parmlib data sets, example: SYS1.PARMLIB(BPXPRMxx), for the following UNIX Parameter Keywords and Values:

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST (optional) /etc/steplib
If specified will use the above value.
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID or (SETUID (for Vendor-provided files)) &
SECURITY (Specified regardless of Vendor-provided or not)
STARTUP_PROC OMVS

c) If the required parameter keywords and values are defined, there is NO FINDING.

d) If the required parameter keywords and values are not defined, this is a FINDING.

Fix Text: Review the settings in PARMLIB member BPXPRMxx for z/OS UNIX security parameters and ensure that the values conform to the specifications below:

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUIDSETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS

BPXPRMxx is the SYS1.PARMLIB member that contains the parameters that control the z/OS UNIX environment. BPXPRMxx controls the way features work and it establishes logical access to data by configuring the HFS environment.

The SUPERUSER parameter specifies the userid to be assigned to users when the su command is entered without a userid operand. The userid must be defined to the ACP as BPXROOT and have a UID of 0.

The TTYGROUP parameter specifies the group name assigned to pseudo terminals (PTYs) and remote terminals (RTYs). The group must be defined to the ACP with a unique GID and users must not be assigned to this group. This group name is used by some shell commands (e.g., talk and write) when writing to the PTY or RTY being used by another user. The name TTY must be used.

The STEPLIBLIST parameter specifies the pathname of the HFS file that contains the list of MVS data sets that are used as step libraries for programs that have the set-user-id or set group id permission bit set. The use of STEPLIBLIST is at the site's discretion, but if used the value of STEPLIBLIST will be /etc/steplib. All update and alter access to the MVS data sets in the list will be logged and only systems programming personnel will be authorized to update the data sets.

The USERIDALIASTABLE parameter specifies the pathname of the HFS file that contains a list of userids and group names with their corresponding alias names. The alias table is intended primarily for use where mixed or lower case userids are used in the UNIX environment. Because the z/OS/ MVS components support only upper case userids, the USERIDALIASTABLE will not be used.

The ROOT parameter specifies data for the file system that is to be mounted as the root file system for z/OS UNIX. ROOT can have a number of sub-parameters; the FILESYSTEM and SETUID|NOSETUID sub-parameters have security considerations. FILESYSTEM can be used to specify the name of the MVS HFS data set that holds the root file system. As the highest point in the HFS hierarchy, this file system is critical to system operations. Therefore appropriate ACP access rules must be written to protect the named data set. Update and alter access must be restricted to the z/OS UNIX kernel and individual systems programming personnel. The SETUID|NOSETUID sub-parameter specifies whether or not the set-user-ID or set-group-ID permission bits are supported. SETUID|NOSETUID also impacts the APF authorized and program-controlled extended attributes. For the root file system, SETUID must be specified for normal operations.

The MOUNT parameter specifies data for a file system that is to be mounted by z/OS UNIX. There are usually multiple MOUNT statements and each can have a number of sub-parameters. The FILESYSTEM, SETUID|NOSETUID, and SECURITY|NOSECURITY sub-parameters have significant security considerations. FILESYSTEM can be used to specify the name of the MVS HFS data set that holds the logical file system. Appropriate ACP access rules must be written to protect the named data set. Update and alter access must be restricted to the z/OS UNIX kernel and to individual systems programming personnel. The SETUID|NOSETUID sub parameter specifies whether or not the set-user-ID or set group ID permission bits are supported. SETUID|NOSETUID also impacts the APF authorized and program-controlled extended attributes. SETUID may be specified for those file systems that contain only vendor-provided software or that have been documented to the IAO as requiring this support. Otherwise NOSETUID must be specified. The SECURITY|NOSECURITY sub-parameter specifies whether security checks are performed. SECURITY must be specified unless a specific exception for the file system has been identified and documented to the IAO. Regardless of IBM defaults, the values for SETUID|NOSETUID and SECURITY|NOSECURITY must be explicitly coded to protect against potential vendor changes and to simplify security reviews.

The STARTUP_PROC parameter specifies the name of the JCL procedure (PROC) that starts the z/OS UNIX component. This started task must be defined to the ACP. The name OMVS must be used.

CCI: CCI-000366

Group ID (Vulid): V-6946

Group Title: ZUSS0013

Rule ID: SV-7247r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0013](#)

Rule Title: z/OS UNIX HFS MapName files security parameters are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

The Systems Programmer will ensure that if the /etc/auto.master HFS FILE is used that each /etc/mapname file listed specifies setuid no and security yes, unless a letter justifying a specific exception is filed with the IAO.

a) Use Vanguard Analyzer option 3-Online Displays, Parmlib Analysis option L. Browse the BPXPRMxx members

b) Review the logical parmli data sets, example: SYS1.PARMLIB(BPXPRMxx), for the following FILESYSTYPE entry:

FILESYSTYPE TYPE(AUTOMNT) ENTRYPOINT(BPXTAMD)

If the above entry is not found or is commented out in the BPXPRMxx member(s), this is NOT APPLICABLE.

NOTE: The /etc/auto.master HFS file (and the use of Automount) is optional. If the file does not exist, this is NOT APPLICABLE.

NOTE: The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified and not allowed to default.

c) If each MapName file specifies the setuid No and security Yes statements for each automounted directory, there is NO FINDING.

d) If there is a deviation from the required values and documentation for the deviation exists, there is NO FINDING.

NOTE: security No disables security checking for file access. Security No is only allowed on test and development domains. setuid Yes allows a user to run under a different UID/GID identity. Justification documentation is required to validate the use of setuid Yes.

e) If (c), or (d) above is untrue, this is a FINDING.

Fix Text: Review the settings in /etc/auto.master and /etc/mapname for z/OS UNIX security parameters and ensure that the values conform to the specifications below.

The /etc/auto.master HFS file (and the use of Automount) is optional.

The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified and not be allowed to default.

Each MapName file will specify the setuid NO and security YES statements for each automounted directory

If there is a deviation from the required values, documentation must exist for the deviation.

Security NO disables security checking for file access. Security NO is only allowed on test and development domains.

Setuid YES allows a user to run under a different UID/GID identity. Justification documentation is required to validate the use of setuid YES.

CCI: CCI-001762

Group ID (Vulid): V-6947

Group Title: ZUSS0014

Rule ID: SV-7248r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0014](#)

Rule Title: z/OS UNIX security parameters for restricted network service(s) in /etc/inetd.conf are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

The Systems Programmer or IAO will ensure that the restricted network services specified in the /etc/inetd.conf file listed in the table below are disabled, unless a letter justifying the use of the restricted network service is on file with the IAO.

RESTRICTED NETWORK SERVICES

| Service | Port |
|------------|------|
| Chargen | 19 |
| Daytime | 13 |
| Discard | 9 |
| Echo | 7 |
| Exec | 512 |
| finger | 79 |
| shell | 514 |
| time | 37 |
| login | 513 |
| smtp | 25 |
| timed | 525 |
| nameserver | 42 |
| systat | 11 |
| uucp | 540 |
| netstat | 15 |
| talk | 517 |
| qotd | 17 |
| tftp | 69 |

b) If all the services in the table above are not found in or are commented out of the /etc/inetd.conf file, there is NO FINDING.

c) If any of the Restricted Network Services defined above is specified, this is a FINDING.

Fix Text: Review the settings in The /etc/inetd.conf file determine if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures.

The following services must be disabled in /etc/inetd.conf unless justified and documented with the IAO:

RESTRICTED NETWORK SERVICES

| Service | Port |
|---------|------|
| Chargen | 19 |

| | |
|------------|-----|
| Daytime | 13 |
| Discard | 9 |
| Echo | 7 |
| Exec | 512 |
| finger | 79 |
| shell | 514 |
| time | 37 |
| login | 513 |
| smtp | 25 |
| timed | 525 |
| nameserver | 42 |
| systat | 11 |
| uucp | 540 |
| netstat | 15 |
| talk | 517 |
| qotd | 17 |
| tftp | 69 |

`/etc/inetd.conf`

The `/etc/inetd.conf` file is used by the INETD daemon. It specifies how INETD is to handle service requests on network sockets. Specifically, there is one entry in `inetd.conf` for each service. Each service entry specifies several parameters. The `login_name` parameter is of special interest. It specifies the userid under which the forked daemon is to execute. This userid is defined to the ACP and it may require a UID(0) (i.e., superuser authority) value.

CCI: CCI-000382

CCI: CCI-001762

Group ID (Vulid): V-6961

Group Title: ZUSS0015

Rule ID: SV-7262r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0015](#)

Rule Title: z/OS UNIX security parameters in `etc/profile` are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(EPROF)

b) If the final or only instance of the UMASK command in /etc/profile is specified as umask 077 , there is NO FINDING.

c) If the LOGNAME variable is marked read-only (i.e., readonly LOGNAME) in /etc/profile, there is NO FINDING.

d) If (b) or(c) above is untrue, this is a FINDING.

Fix Text: Verify that the UMASK command is executed with a value of 077 and the LOGNAME variable is marked read-only for the /etc/profile file, exceptions are documented with the IAO.

The /etc/profile file is the system-wide profile that is executed for each user s shell invocation. It provides a default environment for users. It sets environment variables and executes commands. Although there are several variables and commands that can be included, those with notable security considerations are the STEPLIB variable and the UMASK command. The STEPLIB variable should be assigned a value of none in /etc/profile unless a specific requirement for another value exists. The use of STEPLIB must be coordinated with the SYS1.PARMLIB(BPXPRMxx) STEPLIBLIST control, the /etc/steplib file, and the use of RTLS. The umask command must be executed in /etc/profile with a value of 077. This sets the file-creation permission-code mask so that a file creator has full permissions, group members have no permission, and other users have no permission. Exceptions to this may occur during software installation when the installation process demands a more permissive value, during database access by users, and during administrative actions. All requirements will be justified and documented with the IAO.

CCI: CCI-000366

Group ID (Vulid): V-6963

Group Title: ZUSS0016

Rule ID: SV-7264r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0016](#)

Rule Title: z/OS UNIX security parameters in /etc/rc not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(ERC)

b) If all of the CHMOD commands in /etc/rc do not result in less restrictive access than what is specified in the SYSTEM DIRECTORY SECURITY SETTINGS Table and the SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum, there is NO FINDING.

NOTE: The use of CHMOD commands in /etc/rc is required in most environments to comply with the required settings, especially for dynamic objects such as the /dev directory.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwX | (least restrictive) |
| 6 | rw- | |
| 3 | -wX | |
| 2 | -w- | |
| 5 | r-X | |
| 4 | r-- | |
| 1 | --X | |
| 0 | --- | (most restrictive) |

c) If all of the CHAUDIT commands in /etc/rc do not result in less auditing than what is specified in the SYSTEM DIRECTORY SECURITY SETTINGS Table and the SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum, there is NO FINDING.

NOTE: The use of CHAUDIT commands in /etc/rc may not be necessary. If none are found, there is NO FINDING.

The possible audit bits settings are as follows:

- f log for failed access attempts
- a log for failed and successful access
- no auditing

d) If the `_BPX_JOBNAME` variable is appropriately set (i.e., to match daemon name) as each daemon (e.g., `syslogd`, `inetd`) is started in `/etc/rc`, there is NO FINDING.

NOTE: If `_BPX_JOBNAME` is not specified, the started address space will be named using an inherited value. This could result in reduced security in terms of operator command access.

e) If (b), (c), or (d) above is untrue, this is a FINDING.

Fix Text: Review the settings in the `/etc/rc`. The `/etc/rcfile` is the system initialization shell script. When z/OS UNIX kernel services start, `/etc/rc` is executed to set file permissions and ownership for dynamic system files and to perform other system startup functions such as starting daemons. There can be many commands in `/etc/rc`. There are two specific guidelines that must be followed:

Verify that The `CHMOD` or `CHAUDIT` command does not result in less restrictive security than what is specified in the table in the z/OS STIG addendum under the `SYSTEM DIRECTORY SECURITY SETTINGS`,

Immediately prior to each command that starts a daemon, the `_BPX_JOBNAME` variable must be set to match the daemon s name (e.g., `inetd`, `syslogd`). The use of `_BPX_USERID` is at the site s discretion, but is recommended.

CCI: CCI-000366

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-6968

Group Title: ZUSS0021

Rule ID: SV-7404r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0021](#)

Rule Title: BPX resource(s)s is(are) not protected in accordance with security requirements.

Vulnerability Discussion: z/OS UNIX ACP-defined resources consist of sensitive capabilities including SUPERUSER, daemon, and numerous file manipulation privileges. Missing or inaccurate protection of these resources could allow a user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Responsibility: Systems Programmer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(FACILITY)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0021)

b) Review the following items for the FACILITY resource class, TYPE(FAC):

- 1) The ACF2 rules for the BPX resource specify a default access of NONE.
- 2) There are no ACF2 rules that allow access to the BPX resource.
- 3) There is no ACF2 rule for BPX.SAFFASTPATH defined.
- 4) The ACF2 rules for each of the BPX resources listed in the General Facility Class BPX Resources Table, in the z/OS STIG Addendum, specify a default access of NONE.
- 5) The ACF2 rules for each of the BPX resources listed in the General Facility Class BPX Resources Table, in the z/OS STIG Addendum, restrict access to appropriate system tasks or systems programming personnel.

c) If any item in (b) is untrue, this is a FINDING.

d) If all items in (b) are true, this is NOT A FINDING.

Fix Text: The Systems Programmer and IAO will ensure that BPX. Resources are properly protected and access is restricted to appropriate system tasks or systems programming personnel.

Ensure the following items for the FACILITY resource class, TYPE(FAC):

- 1) The ACF2 rules for the BPX resource specify a default access of NONE.

Example:

```
$KEY(BPX) TYPE(FAC)  
- UID(*) PREVENT
```

- 2) There are no ACF2 rules that allow access to the BPX resource.

Example:

```
$KEY(BPX) TYPE(FAC)  
- UID(*) PREVENT
```

- 3) There is no ACF2 rule for BPX.SAFFASTPATH defined.

Example:

```
$KEY(BPX) TYPE(FAC)  
SAFFASTPATH UID(*) PREVENT
```

- 4) The ACF2 rules for each of the BPX resources listed in the General Facility Class BPX Resources Table, in the zOS STIG Addendum, specify a default access of NONE.

Example:

```
$KEY(BPX) TYPE(FAC)  
DAEMON UID(*) PREVENT  
DEBUG UID(*) PREVENT  
FILEATTR.APF UID(*) PREVENT  
FILEATTR.PROGCTL UID(*) PREVENT  
JOBNAME UID(*) PREVENT  
SAFFASTPATH UID(*) PREVENT  
SERVER UID(*) PREVENT  
SMF UID(*) PREVENT  
STOR.SWAP UID(*) PREVENT  
SUPERUSER UID(*) PREVENT  
WLMSEVER UID(*) PREVENT
```

- 5) The ACF2 rules for each of the BPX resources listed in the General Facility Class BPX Resources Table, in the zOS STIG Addendum, restrict access to appropriate system tasks or systems programming personnel as specified.

Example:

```
$KEY(BPX) TYPE(FAC)
DAEMON UID(*****STC*****FTPD) SERVICE(READ) LOG
DAEMON UID(*****STC*****INETD) SERVICE(READ) LOG
DAEMON UID(*****STC*****NAMED) SERVICE(READ) LOG
DAEMON UID(*****STC*****OMVSKERN) SERVICE(READ) LOG
DAEMON UID(*****STC*****OMVS) SERVICE(READ) LOG
DAEMON UID(*****STC*****OROUTED) SERVICE(READ) LOG
DAEMON UID(*****STC*****OSNMPD) SERVICE(READ) LOG
```

CCI: CCI-000213

CCI: CCI-001764

Group ID (Vulid): V-6970

Group Title: ZUSS0022

Rule ID: SV-19746r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ZUSS0022](#)

Rule Title: z/OS UNIX resources must be protected in accordance with security requirements.

Vulnerability Discussion: z/OS UNIX ACP-defined resources consist of sensitive capabilities including SUPERUSER, daemon, and numerous file manipulation privileges. Missing or inaccurate protection of these resources could allow a user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(SURROGAT)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0022)
- b) If the ACF2 rules for all BPX.SRV.user TYPE(SUR) resources specify a default access of NONE, there is NO FINDING.
- c) If the ACF2 rules for all BPX.SRV.user TYPE(SUR) resources restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX, there is NO FINDING.
- d) If (b) or (c) above is untrue, this is a FINDING.

Fix Text: a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(SURROGAT)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0022)
- b) If the ACF2 rules for all BPX.SRV.user TYPE(SUR) resources specify a default access of NONE, there is NO FINDING.
- c) If the ACF2 rules for all BPX.SRV.user TYPE(SUR) resources restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX, there is NO FINDING.
- d) If (b) or (c) above is untrue, this is a FINDING.
- 1) RACF rules for all BPX.SRV.user SURROGAT resources must specify a default access of NONE.

A sample is provided here:

RDEF SURROGAT BPX.SRV.user UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))

- 2) RACF rules for all BPX.SRV.user SURROGAT resources must restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX.

RDEF SURROGAT BPX.SRV.user UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
PE BPX.SRV.user CL(SURROGAT) ID(<server>)

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-6972

Group Title: ZUSS0023

Rule ID: SV-19748r3_rule

Severity: CAT I

Rule Version (STIG-ID): [ZUSS0023](#)

Rule Title: z/OS UNIX SUPERUSER resource must be protected in accordance with guidelines.

Vulnerability Discussion: z/OS UNIX ACP-defined resources consist of sensitive capabilities including SUPERUSER, daemon, and numerous file manipulation privileges. Missing or inaccurate protection of these resources could allow a user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(UNIXPRIV)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0023)

b) Review the following items for the UNIXPRIV resource class, TYPE(UNI):

- 1) The ACF2 rules for the SUPERUSER resource specify a default access of NONE.
 - 2) There are no ACF2 rules that allow access to the SUPERUSER resource.
 - 3) There is no ACF2 rule for CHOWN.UNRESTRICTED defined.
 - 4) The ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS STIG Addendum, specify a default access of NONE.
 - 5) The ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS STIG Addendum, restrict access to appropriate system tasks or systems programming personnel.
- c) If any item in (b) is untrue, this is a FINDING.
- d) If all items in (b) are true, this is NOT A FINDING.

Fix Text: The IAO will ensure that all SUPERUSER resources for the UNIXPRIV resource class are restricted to appropriate system tasks and/or system programming personnel.

The ACF2 rules for the SUPERUSER resource specify a default access of NONE.

There are no ACF2 rules that allow access to the SUPERUSER resource.

There is no ACF2 rule for CHOWN.UNRESTRICTED defined.

The ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS STIG Addendum, specify a default access of NONE.

The ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS STIG Addendum, restrict access to appropriate system tasks or systems programming personnel.

Example:

```
SET R(UNI)
$KEY(SUPERUSER) TYPE(UNI)
$MEMBER(SUPRUSER)
FILESYS UID(syspau) LOG
FILESYS.CHOWN UID(syspau) LOG
FILESYS.MOUNT UID(syspau) LOG
FILESYS.PFCTL UID(syspau) LOG
FILESYS.VREGISTER UID(syspau) LOG
IPC.RMID UID(syspau) LOG
PROCESS.GETPSENT UID(syspau) LOG
PROCESS.KILL UID(syspau) LOG
```


PROCESS.PTRACE UID(syspau) LOG
SETPRIORITY UID(syspau) LOG
- UID(*) PREVENT

CCI: CCI-000213

CCI: CCI-001764

Group ID (Vulid): V-6974

Group Title: ZUSS0031

Rule ID: SV-7277r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0031](#)

Rule Title: z/OS UNIX MVS data sets or HFS objects are not properly protected.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- PARMLIB(BPXPRMxx)

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(HFSRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0031)

b) If the ACP data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update access to the z/OS UNIX kernel (i.e., OMVS or OMVSKERN) there is NO FINDING.

c) If the ACP data set rules for the data set referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update and/or allocate access to systems programming personnel there is NO FINDING.

d) If (b) or (c) above is untrue, this is a FINDING.

Fix Text: Review the access authorizations defined in the ACP for the MVS data sets that contain operating system components and for the MVS data sets that contain HFS file systems and ensure that they conform to the specifications below Review the UNIX permission bits on the HFS directories and files and ensure that they conform to the specifications below:

The ACP data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update access to the z/OS UNIX kernel (i.e., OMVS or OMVSKERN

The ACP data set rules for the data set referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update and/or allocate access to systems programming personnel

The ROOT parameter specifies data for the file system that is to be mounted as the root file system for z/OS UNIX. ROOT can have a number of sub-parameters; the FILESYSTEM and SETUID|NOSETUID sub-parameters have security considerations. FILESYSTEM can be used to specify the name of the MVS HFS data set that holds the root file system. As the highest point in the HFS hierarchy, this file system is critical to system operations. Therefore appropriate ACP access rules must be written to protect the named data set. Update and alter access must be restricted to the z/OS UNIX kernel and individual systems programming personnel. The SETUID|NOSETUID sub-parameter specifies whether or not the set-user-ID or set-group-ID permission bits are supported. SETUID|NOSETUID also impacts the APF authorized and program-controlled extended attributes. For the root file system, SETUID must be specified for normal operations.

The MOUNT parameter specifies data for a file system that is to be mounted by z/OS UNIX. There are usually multiple MOUNT statements and each can have a number of sub-parameters. The FILESYSTEM, SETUID|NOSETUID, and SECURITY|NOSECURITY sub-parameters have significant security considerations. FILESYSTEM can be used to specify the name of the MVS HFS data set that holds the logical file system. Appropriate ACP access rules must be written to protect the named data set. Update and alter access must be restricted to the z/OS UNIX kernel and to individual systems programming personnel. The SETUID|NOSETUID sub parameter specifies whether or not the set-user-ID or set group ID permission bits are supported. SETUID|NOSETUID also impacts the APF authorized and program-controlled extended attributes. SETUID may be specified for those file systems that contain only vendor-provided software or that have been documented to the IAO as requiring this support. Otherwise NOSETUID must be specified. The SECURITY|NOSECURITY sub-parameter specifies whether security checks are performed. SECURITY must be specified unless a specific exception for the file system has been identified and documented to the IAO. Regardless of IBM defaults, the values for SETUID|NOSETUID and SECURITY|NOSECURITY must be explicitly coded to protect against potential vendor changes and to simplify security reviews.

Security rules must be defined to prevent unauthorized changes to the z/OS UNIX components in MVS data sets. Because z/OS UNIX is integrated with the z/OS base control program, many of the z/OS UNIX components reside in data sets that are protected by security definitions specified elsewhere. The data set names (or masks) unique to z/OS UNIX that may require additional definitions are listed in this section. Data sets in conventional MVS formats (e.g., PDS) and those in HFS format are listed. There is also a note on security for user MVS data sets in HFS format.

The following HFS format data sets are unique to z/OS UNIX and require security definitions:

MVS DATA SETS CONTAINING HFS DATA

| DATA SET NAME/MASK | MAINTENANCE TYPE |
|--------------------|------------------|
|--------------------|------------------|

| | |
|------------------|--------|
| SYS1.OE.ROOT | Target |
| SYS3.OE.ETCFILES | Target |

These data sets should have all access restricted to systems programming personnel and to the z/OS UNIX kernel userid OMVS. The site may choose different names for these data sets, but the access restrictions must be maintained.

There may be additional data sets that contain system HFS data. Any data set that specifies a file system that is at the root level (e.g., /tmp, /u) must also have all access restricted to systems programming personnel and to the z/OS UNIX kernel userid.

Depending on the number of users defined in a given z/OS UNIX image, there may be a need to define individual MVS data sets to hold their personal HFS format data. These data sets must be protected in accordance with the existing security guidelines for user data. However, there is a need for special additions to those rules. The z/OS UNIX kernel userid OMVS must have update access to all user HFS data sets. Also, users must not have update access to the MVS data sets so that HFS permission controls cannot be altered outside of the z/OS UNIX environment.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-6976

Group Title: ZUSS0032

Rule ID: SV-7279r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0032](#)

Rule Title: z/OS UNIX MVS data sets WITH z/OS UNIX COMPONENTS are not properly protected

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the ACP Data Collection:

- SENSITIVE.RPT(USSRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0032)

b) If the ACP data set rules for each of the data sets listed in the MVS DATA SETS WITH z/OS UNIX COMPONENTS Table in the z/OS STIG Addendum restrict UPDATE and ALLOCATE access to systems programming personnel, there is NO FINDING.

c) If (b) above is untrue, this is a FINDING.

Fix Text: Verify that the ACP data set rules for each of the data sets listed in the specified table in the z/OS STIG Addendum under MVS DATA SETS WITH z/OS UNIX COMPONENTS restrict UPDATE and ALLOCATE access to systems programming personnel.

The data sets designated as distribution data sets should have all access restricted to systems programming personnel. TSO/E users who also use z/OS UNIX should have read access to the SYS1.SBPX* data sets. Read access for all users to the remaining target data sets is at the site's discretion. All other access must be restricted to systems programming personnel.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-6977

Group Title: ZUSS0033

Rule ID: SV-7280r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0033](#)

Rule Title: z/OS UNIX MVS data sets used as step libraries in /etc/steplib are not properly protected

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(STLLRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZUSS0033)

___ The ACP data set rules for libraries specified in the STEPLIBLIST file allow inappropriate access.

___ The ACP data set rules for libraries specified in the STEPLIBLIST file do not restrict UPDATE and/or ALTER/ALLOCATE access to only systems programming personnel.

___ The ACP data set rules for libraries specified in the STEPLIBLIST file do not specify that all (i.e., failures and successes) UPDATE and/or ALTER/ALLOCATE access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: Verify with the IAO that update and allocate access to libraries residing in the /etc/steplib is limited to system programmers only.

The STEPLIBLIST parameter specifies the pathname of the HFS file that contains the list of MVS data sets that are used as step libraries for programs that have the set-user-id or set group id permission bit set. The use of STEPLIBLIST is at the site's discretion, but if used the value of STEPLIBLIST will be /etc/steplib. All update and alter access to the MVS data sets in the list will be logged and only systems programming personnel will be authorized to update the data sets.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-6978

Group Title: ZUSS0034

Rule ID: SV-7281r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0034](#)

Rule Title: z/OS UNIX HFS permission bits and audit bits for each directory will be properly protected or specified.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(SDPERM)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ZUSS0034)

The HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the SYSTEM DIRECTORY SECURITY SETTINGS Table in the z/OS STIG Addendum. If the guidance is true, this is not a finding.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

- 7 rwx (least restrictive)

| | | |
|---|-----|--------------------|
| 6 | rw- | |
| 3 | -wx | |
| 2 | -w- | |
| 5 | r-x | |
| 4 | r-- | |
| 1 | --x | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on each of the HFS directory in the table in the z/OS STIG Addendum under the SYSTEM DIRECTORY SECURITY SETTINGS, are equal or more restrictive.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwx | (least restrictive) |
| 6 | rw- | |
| 3 | -wx | |
| 2 | -w- | |
| 5 | r-x | |
| 4 | r-- | |
| 1 | --x | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

The following commands are a sample of the commands to be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 0755 /
chaudit w=sf,rx+f /
chmod 0755 /bin
```

chaudit rwx=f /bin

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-6979

Group Title: ZUSS0035

Rule ID: SV-7282r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0035](#)

Rule Title: z/OS UNIX SYSTEM FILE SECURITY SETTINGS will be properly protected or specified.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(SDPERM)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ZUSS0034)

The HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the SYSTEM DIRECTORY SECURITY SETTINGS Table in the z/OS STIG Addendum. If the guidance is true, this is not a finding.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwX | (least restrictive) |
| 6 | rw- | |
| 3 | -wX | |
| 2 | -w- | |
| 5 | r-X | |
| 4 | r-- | |
| 1 | --X | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS files listed in the SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum.

There are a number of files that must be secured to protect system functions in z/OS UNIX. Where not otherwise specified, these files must receive a permission setting of 744 or 774. The 774 setting may be used at the site s discretion to help to reduce the need for assignment of superuser privileges. The table identifies permission bit and audit bit settings that are required for these specific files. More restrictive permission settings may be used at the site s discretion or as specific environments dictate.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwX | (least restrictive) |
| 6 | rw- | |
| 3 | -wX | |
| 2 | -w- | |
| 5 | r-X | |
| 4 | r-- | |
| 1 | --X | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

The following commands are a sample of the commands to be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1755 /bin/sh
chaudit w=sf,rx+f /bin/sh
chmod 0740 /dev/console
chaudit rwx=f /dev/console
```

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-6981

Group Title: ZUSS0036

Rule ID: SV-7284r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0036](#)

Rule Title: z/OS UNIX MVS HFS directory(s) with "other" write permission bit set are not properly defined.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, DCSL-1, ECCD-1, ECCD-2

Check Content:

The Systems Programmer will ensure that the HFS directory(ies) with the "other" write permission bit set is (are) not properly defined.

a) If there are no directories that have the other write permission bit set on without the sticky bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a t or T in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be drwxrwxrwt .

b) If all directories that have the other write permission bit set on do not contain any files with the setuid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an s or S in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be -rwsrwxrwx .

c) If all directories that have the other write permission bit set on do not contain any files with the setgid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an s or S in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be -rwxrwsrwx .

d) If (a), (b), or (c) above is untrue, this is a FINDING.

Fix Text: The systems programmer will verify the following:

b) There are no directories that have the other write permission bit set on without the sticky bit set on.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a t or T in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be drwxrwxrwt .

c) All directories that have the other write permission bit set on do not contain any files with the setuid bit set on.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an s or S in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be -rwsrwxrwx .

d) All directories that have the other write permission bit set on do not contain any files with the setgid bit set on.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an s or S in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be -rwxrwsrwx .

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6985

Group Title: ZUSS0041

Rule ID: SV-7288r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0041](#)

Rule Title: Attributes of z/OS UNIX user accounts are not defined properly

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2

Check Content:

Refer to the following report produced by the ACP Data Collection:

ACF2

- ACF2CMDS.RPT(OMVSGRP)

RACF

- RACFCMDS.RPT(LISTGRP)

TSS

- TSSCMDS.RPT(OMVSUSER)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZUSS0041)

NOTE: A site can choose to have both an OMVSGRP group and an STCOMVS group or combine the groups under one of these names.

Ensure that the OMVSGRP and/or STCOMVS groups are defined and have a unique GID in the range of 1-99.

Fix Text: The Systems Programmer will ensure that the OMVSGRP group and / or the STCOMVS group are each defined to the security database with a unique GID in the range of 1-99.

OMVSGRP is the name suggested by IBM for all the required userids. STCOMVS is the standard name used at some sites for the userids that are associated with z/OS UNIX started tasks and daemons. These groups can be combined at the site s discretion.

CCI: CCI-000764

Group ID (Vulid): V-6986

Group Title: ZUSS0042

Rule ID: SV-7289r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0042](#)

Rule Title: z/OS UNIX each group is not defined with a unique GID.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

Refer to the following report produced by the ACP Data Collection:

ACF2

- ACF2CMDS.RPT(OMVSGRP)

RACF

- RACFCMDS.RPT(LISTGRP)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZUSS0042)

For ACF2 and RACF ensure that each GID is unique to a specific group.

For TSS this is Not Applicable.

Fix Text: The systems programmer will verify that each group has a unique GID number,

CCI: CCI-000764

Group ID (Vulid): V-6987

Group Title: ZUSS0043

Rule ID: SV-7290r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0043](#)

Rule Title: The user account for the z/OS UNIX kernel (OMVS) is not properly defined to the security database.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

If this is a classified system this is not applicable.

From an ACF2 command line enter:

SET CONTROL(GSO)

SHOW UNIXOPTS

Alternately:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)
- ACF2CMDS.RPT(OMVSUSER)

Note: This check applies to any user identifier (LOGONID) used to model OMVS access on the mainframe. This includes any DFTUSER; MODLUSER and BPX.UNIQUE.USER. If MODLUSER is specified then UNIQUUSER must be specified.

If DFTUSER or MODLUSER is not defined in the UNIXOPTS record there is no finding.

If ALL user identifiers (LOGONID) defined to DFTUSER or MODLUSER. or BPX.UNIQUE.USER user account is defined as follows, there is no finding:

A non-writable HOME directory:
Shell program specified as /bin/echo or /bin/false

Note: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Fix Text: Ensure that the below options are enforced.

Note: This only applies to DFTUSER or MODLUSER or BPX.UNIQUE.USER as appropriate.

Ensure that DFTUSER or MODLUSER or BPX.UNIQUE.USER user account is defined as follows:

A non-writable HOME directory:
Shell program specified as /bin/echo or /bin/false

Note: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Example:
SET PROFILE(USER) DIV(OMVS)
LIST OMVS

INSERT OMVS HOME(/) OMVSPGM(/bin/false) UID(0)

CCI: CCI-000764

Group ID (Vulid): V-6988

Group Title: ZUSS0044

Rule ID: SV-87465r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0044](#)

Rule Title: The user account for the z/OS UNIX SUPERUSER userid must be properly defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

Refer to system PARMLIB member BPXPRMxx (xx is determined by OMVS entry in IEASYS00.)

Determine the user ID identified by the SUPERUSER parameter. (BPXROOT is the default).

From a command input screen enter:

SET LID

LIST LIKE (superuser userid)

If the SUPERUSER userid is defined as follows, this is not a FINDING:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- Default group specified as OMVSGRP or STCOMVS

From a command input screen enter:

SET PROFILE(USER) DIVISION(OMVS)

SET VERBOSE

LIST <superuser userid>

If the SUPERUSER userid is defined as follows, this is not a FINDING:

- UID(0)
- HOME directory specified as /
- Shell program specified as /bin/sh

Alternately,

Refer to the following reports produced by the ACP Data Collection:

- ACF2CMDS.RPT(OMVSUSER)
- ACF2CMDS.RPT(LOGONIDS)

If SUPERUSER userid is defined as follows, this is not a finding:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- Default group specified as OMVSGRP or STCOMVS
- UID(0)
- HOME directory specified as /
- Shell program specified as /bin/sh

Fix Text: Define the user ID identified in the BPXPRM00 SUPERUSER parameter as specified below:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)

- Default group specified as OMVSGRP or STCOMVS
- UID(0)
- HOME directory specified as /
- Shell program specified as /bin/sh

CCI: CCI-000764

Group ID (Vulid): V-6989

Group Title: ZUSS0045

Rule ID: SV-87475r1_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0045](#)

Rule Title: The user account for the z/OS UNIX (RMFGAT) is not properly defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

RMFGAT is the userid for the Resource Measurement Facility (RMF) Monitor III Gatherer. If RMFGAT is not define, this is not applicable.

From a command input screen enter:

SET LID

LIST RMFGAT

If the RMFGAT is defined as follows, this is not a FINDING:

- Default group specified as OMVSGRP or STCOMVS

From a command input screen enter:

SET PROFILE(USER) DIVISION(OMVS)

SET VERBOSE

LIST RMFGAT

If RMFGAT is defined as follows, this is not a finding:

- A unique, non-zero UID

- HOME directory specified as /
- Shell program specified as /bin/sh

Alternately,

Refer to the following reports produced by the ACP Data Collection:

- ACF2CMDS.RPT(OMVSUSER)
- ACF2CMDS.RPT(LOGONIDS)

If RMFGAT is defined as follows, this is not a finding:

- Default group specified as OMVSGRP or STCOMVS
- A unique, non-zero UID
- HOME directory specified as /
- Shell program specified as /bin/sh

Fix Text: Define the RMFGAT user account as specified below:

- Default group specified as OMVSGRP or STCOMVS
- A unique, non-zero UID
- HOME directory specified as /
- Shell program specified as /bin/sh

CCI: CCI-000764

Group ID (Vulid): V-6991

Group Title: ZUSS0046

Rule ID: SV-7294r2_rule

Severity: CAT I

Rule Version (STIG-ID): [ZUSS0046](#)

Rule Title: UID(0) is improperly assigned.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACP Data Collection:

ACF2

- ACF2CMDS.RPT(OMVSUSER)

RACF

- RACFCMDS.RPT(LISTUSER)

TSS

- TSSCMDS.RPT(OMVSUSER)

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZUSS0046)

b) If UID(0) is assigned only to system tasks such as the z/OS/ UNIX kernel (i.e., OMVS), z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons, there is NO FINDING.

c) If UID(0) is assigned to security administrators who create or maintain user account definitions; and to systems programming accounts dedicated to maintenance (e.g., SMP/E) of HFS-based components, there is NO FINDING.

NOTE: The assignment of UID(0) confers full time superuser privileges. This is not appropriate for personal user accounts. Access to the BPX.SUPERUSER resource is used to allow personal user accounts to gain short-term access to superuser privileges.

d) If UID(0) is assigned to non-systems or non-maintenance accounts, this is a FINDING.

Fix Text: The systems programmer will verify that UID(0) is defined as specified below:

UID(0) is assigned only to system tasks such as the z/OS UNIX kernel (i.e., OMVS), z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons.

UID(0) is assigned to security administrators who create or maintain user account definitions; and to systems programming accounts dedicated to maintenance (e.g., SMP/E) of HFS-based components..

NOTE: The assignment of UID(0) confers full time superuser privileges, this is not appropriate for personal user accounts. Access to the BPX.SUPERUSER resource is used to allow personal user accounts to gain short-term access to superuser privileges.

CCI: CCI-000764

CCI: CCI-002235

Group ID (Vulid): V-6992

Group Title: ZUSS0047

Rule ID: SV-7295r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0047](#)

Rule Title: z/OS UNIX user accounts are not properly defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACP Data Collection:

- ACF2
- ACF2CMDS.RPT(OMVSUSER)
- RACF
- RACFCMDS.RPT(LISTUSER)
- TSS
- TSSCMDS.RPT(OMVSUSER)

NOTE: This check only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

b) If each user account is defined as follows, there is NO FINDING:

- 1) A unique UID number (except for UID(0) users)
- 2) A unique HOME directory (except for UID(0) and other system task accounts)
- 3) Shell program specified as /bin/sh , /bin/tcsh , /bin/echo , or /bin/false

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

c) If any user account is not defined as specified in (b) above, this is a FINDING.

Fix Text: The systems programmer will verify that each user account is defined as specified below:

NOTE: This check only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

- 1) A unique UID number (except for UID(0) users)
- 2) A unique HOME directory (except for UID(0) and other system task accounts)
- 3) Shell program specified as /bin/sh , /bin/tcsh , /bin/echo , or /bin/false

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

CCI: CCI-000764

Group ID (Vulid): V-7050

Group Title: ZUSS0048

Rule ID: SV-7940r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0048](#)

Rule Title: Attributes of z/OS UNIX user accounts used for account modeling must be defined in accordance with security requirements.

Vulnerability Discussion: RACF userids that use z/OS UNIX must be properly configured. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

If this is a classified system this is not applicable.

From an ACF2 command line enter:

SET CONTROL(GSO)

SHOW UNIXOPTS

Alternately:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)
- ACF2CMDS.RPT(OMVSUSER)

Note: This check applies to any user identifier (LOGONID) used to model OMVS access on the mainframe. This includes any DFTUSER; MODLUSER and BPX.UNIQUE.USER. If MODLUSER is specified then UNIQUSER must be specified.

If DFTUSER or MODLUSER is not defined in the UNIXOPTS record there is no finding.

If ALL user identifiers (LOGONID) defined to DFTUSER or MODLUSER. or BPX.UNIQUE.USER user account is defined as follows, there is no finding:

A non-writable HOME directory:

Shell program specified as /bin/echo or /bin/false

Note: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Fix Text: Use of the OMVS default UID will not be allowed on any classified system. This is not an issue when using BPX.UNIQUE.USER.

Define user id used for OMVS account modeling with a non-0 UID, a non-writable home directory, such as "\" root, and a non-executable, but existing, binary file, "/bin/false" or /bin/echo.

```
AG OEDFLTG SUPGROUP(ADMIN) OWNER(ADMIN) OMVS(GID(777777))
AU OEDFLTU DFLTGRP(OEDFLTG) NAME('OE DEFAULT USER') NOPASS -
OMVS(UID(99999) HOME('/u/oeflt') PROGRAM('/bin/echo')) -
DATA('DEFAULT OMVSUSERID ADDED WITH SOER5')
RDEF FACILITY BPX.DEFAULT.USER APPLDATA('OEDFLTU/OEDFLTG') -
DATA('ADDED TO SUPPORT THE DEFAULT USER') UACC(NONE) OWNER(ADMIN)
SETR RACLIST(FACILITY) REFRESH
```

CCI: CCI-000764

Group ID (Vulid): V-28603

Group Title: ZUSS0080

Rule ID: SV-36387r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSS0080](#)

Rule Title: z/OS USS Software owning Shared accounts do not meet strict security and creation restrictions.

Vulnerability Discussion: Shared accounts by nature are a violation of proper audit trail and proper user authentication. If not properly controlled, could cause system corruption without an audit trail tracking session activity to an individual user's identity.

Responsibility: Information Assurance Officer

IAControls: ECAR-1, ECAR-2, ECAR-3, IAGA-1

Check Content:

z/OS Software owning Shared accounts maybe created for the installation and upgrades on the z/OS Mainframe products that require the use of USS (UNIX System Services) as long as all IA requirements are met. z/OS USS Software Owning Shared Accounts shall be referenced within this VUL as the full name or abbreviated Shared accounts for all references within this VUL.

Rules and requirements for z/OS USS Software Owning Shared Accounts.

- 1) Shall include a statement from the responsible SA requesting the shared account , stating specific justification for the z/OS USS Software Owning shared account. Responsible SA shall be responsible for maintaining all documentation concerning account, usage, control, annual review, etc and shall provide upon request by IA staff or auditors as requested.
- 2) A separate z/OS USS Software Owning shared account userid will be created for each application and/or product that requires USS for separation of duties for product support. This shared account shall be used for the sole purpose of file/directory ownership based upon the UID assigned to the shared account .
- 3) The shared accounts shall only be used within/for USS (UNIX System Services). The shared account userids shall have no special privileges, will not be granted access to interactive on-line facilities, batch facility, and will not be granted access to datasets and resources outside of the USS environment.
- 4) The shared account userids shall adhere to the same complex password syntax rules and shall be assigned a non-expiring complex password or be set up as protected under RACF.
- 5) Authorized user(s) shall only access shared account via the USS SU Command (switch user: su s userid) and not utilize any password. When the ACP IAO creates the account with a complex password, such password shall not be written down or shared with others.
- 6) The responsible documented z/OS system programmer shall be granted specific limited and temporary access based upon submitted security service requests identifying project, duration required and justification for accessing shared account via the su command on a specific z/OS domain, example: initial software installation or upgrade of specific vendor software.
- 7) Responsible individual z/OS System programmer shall be granted temporary access to the specific BPX.SRV.userid (userid shall be the single shared account requested) in the surrogate user class with full logging of the permission to BPX.SRV.userid for the specific period of time required to perform functional requirements via the su command and appropriate usage of the shared account .
- 8) Standard procedure for all updates within USS Directories/files shall be performed based upon the direct authority granted to the z/OS system programmer individual userids. Shared accounts shall only be utilized for initial software installation or vendor software upgrades.

If all the above requirements are not met for the z/OS USS Software Owning shared account, this is a finding.

Fix Text: To create a shared account follow the instructions below.

Shared accounts will be created for the installation and upgrades on the z/OS Mainframe products that require the use of USS (UNIX System Services)

Rules and requirements for z/OS USS Software Owning Shared Accounts

- 1) Shall include a statement from the responsible SA requesting the shared account , stating specific justification for the z/OS USS Software Owning shared account. Responsible SA shall be responsible for maintaining all documentation concerning account, usage, control, annual review, etc and shall provide upon request by IA staff or auditors as requested.
- 2) A separate z/OS USS Software Owning shared account userid will be created for each application and/or product that requires USS for separation of duties for product support. This shared account shall be used for the sole purpose of file/directory software ownership based upon the UID assigned to the shared account .
- 3) The shared accounts shall only be used within/for USS (UNIX System Services). The shared account userids shall have no special privileges, shall not be granted access to interactive on-line facilities, batch facility, and shall not be granted access to datasets and resources outside of the USS environment.
- 4) The shared account userids shall adhere to the same complex password syntax rules and shall be assigned a non-expiring complex password or be set up as protected under RACF.
- 5) Authorized user(s) shall only access shared account via the USS SU Command (switch user: su s userid) and not utilize any password. When the ACP IAO creates the account with a complex password, such password shall not be written down or shared with others.
- 6) The responsible documented z/OS system programmer shall be granted specific, limited and temporary access based upon submitted security service requests identifying project, duration required and justification for accessing shared account via the su command on a specific z/OS domain, example: initial software installation or upgrade of specific vendor software.
- 7) Responsible Individual z/OS System programmer shall be granted temporary access to the specific BPX.SRV.userid (userid shall be the single shared account requested) in the surrogate user class with full logging of the permission to BPX.SRV.userid for the specific period of time required to perform functional requirements via the su command and appropriate usage of the shared account .
- 8) Standard procedure for all updates within USS Directories/files shall be performed based upon the direct authority granted to the z/OS system programmer individual userids. Shared accounts shall only be utilized for initial software installation or vendor software upgrades.

To share HFS or ZFS Files associated with this shared file :

Associate the directory or file with a ACP group that has been assigned a z/OS UNIX group identifier (GID), give the ACP group the appropriate group permissions, and connect the users to this ACP group

With z/OS Version 1 Release 3 or later, you can use access control lists (ACLs) to control access to files and directories by individual UIDs and GIDs. With ACLs, you can give more than one group permissions for directories or files on HFS, so you do not need to ensure that all your file owners connect to the same ACP group.

NOTE: If using HFSSEC for TSS or ACF2 you will not be able to use ACLs to control access to your files.

Both CA-ACF2 and CA-TSS provide for a feature and capability to control all HFS/ZFS files and directories directly within the ACP using HFSSEC resource class. HFSSEC provides full control, auditing and review capability within the native ACP software and requires less interaction in setting up appropriate and proper access controls over the vast USS environment. With appropriate HFSSEC controls in place, access controls are performed by the ACP and not via USS UID/GID Controls. Using HFSSEC, all controls are at the userid level and would not be able to utilize ACL s to control access.

CCI: CCI-000213

CCI: CCI-000770

Group ID (Vulid): V-6997

Group Title: ZUSSA050

Rule ID: SV-7300r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSSA050](#)

Rule Title: The z/OS Default profiles must not be defined in the corresponding FACILITY Class Profile for classified systems.

Vulnerability Discussion: The ACF2 FACILITY Class BPX. UNIQUE.USER profile contains the userid or the userid/group ID of the default profiles to be used for a user without a z/OS UNIX profile (i.e., OMVS Segment). In classified system user access will not be determined by default.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

If this is an Unclassified system this is not applicable.

From ACF2 Command Line enter:

Set CONTROL(GSO)

Show UNIXOPTS

Alternately:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)

- Classification of System

Automated Analysis:

Refer to the following report produced by the ACF2 Data Collection:

- PDI(ZUSSA050)

If system is classified the UNIXOPTS record specifies DFTGROUP(); DFTUSER(); NOUNIQUEUSER AND MODLUSER(), there is no finding.

Fix Text: Ensure that UNIXOPTS record does not specify DFTGROUP and DFTUSER fields for classified systems.

Ensure that then UNIXOPTS record specifies NOUNIQUEUSER and no MODLUSER

If system is classified the UNIXOPTS record must specify DFTGROUP(); DFTUSER() and MODLUSER(). NOUNIQUEUSER must be specified.

Example:

SET C(GSO)

LIST UNIXOPTS

CHOWNRES DFTGROUP() DFTUSER() NODIRACC
NODIRSRCH NOFSOBJ NOFSSEC NOGOSETGID NOHFSACL NOHFSSEC
NOIPCOBJ NGROUPS(300) NOPROCACT NOPROCESS MODLUSER() NOUNIQUEUSER

CCI: CCI-000366

Group ID (Vulid): V-6994

Group Title: ZUSSA053

Rule ID: SV-7297r3_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSSA053](#)

Rule Title: The GSO UNIXOPTS record must specify CHOWNRES.

Vulnerability Discussion: Parameter settings in the ACP impact the security level of z/OS UNIX.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

For CA-ACF2 Release 15 and above this is not applicable.

Refer to the following report produced by the ACF2 Data Collection.

- ACF2CMDS.RPT(ACFGSO)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection:

- PDI(ZUSSA053)

If the UNIXOPTS record does not specify CHOWNRES this is a finding.

Fix Text:

The IAO must set the GSO UINIXOPTS record to specify CHOWNRES.

Example:

```
SET C(GSO)
LIST UNIXOPTS
```

```
CHOWNRES DFTGROUP(OMVSDGRP) DFTUSER(OMVSUSER) NODIRACC
NODIRSRCH NOFSOBJ NOFSSEC NOGOSETGID NOHFSACL NOHFSSEC
NOIPCOBJ NGROUPS(300) NOPROACT NOPROCESS
```

CCI: CCI-000366

CCI: CCI-001499

Group ID (Vulid): V-6998

Group Title: ZUSSA060

Rule ID: SV-7301r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSSA060](#)

Rule Title: The RACF Classes required to properly security the z/OS UNIX environment are not ACTIVE.

Vulnerability Discussion: The FACILITY, SURROGAT, and UNIXPRIV Class support profiles used to secure the z/OS UNIX (OMVS) environment. Without these classes being in an ACTIVE status, system integrity can be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMD5.RPT(ACFGSO)

Automated Analysis

Refer to the following report produced by the ACF2 Data Collection:

- PDI(ZUSSA060)

b) If the CLASMAP DEFINITIONS list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes, there is NO FINDING.

NOTE: The TYPE CODE values should be FAC, SUR, and UNI.

c) If (b) is untrue, this is a FINDING.

Fix Text: The IAO will ensure that the CLASMAP DEFINITIONS list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes.

Ensure the CLASMAP DEFINITIONS list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes. .

NOTE: The TYPE CODE values should be FAC, SUR, and UNI.

Example:

TSO ACF
SHOW CLASMAP

CCI: CCI-000213

Group ID (Vulid): V-6999

Group Title: ZUSSAR070

Rule ID: SV-7302r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZUSSA070](#)

Rule Title: RACF Classes required to support z/OS UNIX security are not properly implemented with the SETROPTS RACLIST command.

Vulnerability Discussion: RACF provides the ability to load certain class profiles into memory for better performance thru the use of the SETR RACLIST command. For some classes, RACLISTing is strongly recommended and should be implemented. By not following vendor recommendations, unpredictable results could occur that compromise the integrity of the z/OS system.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZUSSA070)

b) If the INFODIR record includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes, there is NO FINDING.

NOTE: The TYPES should be R-RFAC, R-RSUR, and R-RUNI. The use of the R- prefix that indicates the rules are resident is recommended, not required.

c) If (b) is untrue, this is a FINDING.

Fix Text: The IAO will ensure that the INFODIR record includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes.

Ensure the INFODIR record includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes, there is NO FINDING.

NOTE: The TYPES should be R-RFAC, R-RSUR, and R-RUNI. The use of the R- prefix that indicates the rules are resident is recommended, not required.

Example:

SET C(GSO)
LIST INFODIR

TYPES(R-PCMF R-PGRP R-PUSR R-RAPL R-RCAC R-RCAT R-RCLS
R-RCMF R-RDLF R-RDSO R-RFAC R-RIOA R-RKT4 R-RMGM R-RMQA
R-ROCS R-ROMS R-ROPR R-ROSM R-ROVS R-RPGM R-RPKC R-RRSY
R-RSAF R-RSDS R-RSER R-RSPL R-RSTR R-RSUR R-RTAC R-RTGR
R-RTKC R-RTPE R-RTPR R-RUNI R-RWTR)

CCI: CCI-000366

Group ID (Vulid): V-6949

Group Title: ZVTM0011

Rule ID: SV-7250r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZVTM0011](#)

Rule Title: The VTAM USSTAB definitions are being used for unsecured terminals

Vulnerability Discussion: VTAM options and definitions are used to define VTAM operational capabilities. They must be strictly controlled. Unauthorized users could override or change start options or network definitions. Failure to properly control VTAM resources could potentially compromise the network operations.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, IAAC-1

Check Content:

a) Refer to the following items gathered from the VTAM Systems Programmer's Worksheet in the Preliminary Information Worksheets in U_zOS_STIG_INSTRUCTION.doc:

- ___ 1. Documentation regarding terminal naming standards.
- ___ 2. Documentation of all procedures controlling terminal logons to the system.
- ___ 3. A complete list of all USS commands used by terminal users to log on to the system.
- ___ 4. A complete list of all terminals and/or terminal types controlled by LOGAPPL definitions only.

___ 5. Members and data set names containing USSTAB and LOGAPPL definitions of all terminals that can log on to the system (e.g., SYS1.VTAMLST).

___ 6. Members and data set names containing logon mode parameters.

b) If USSTAB definitions are only used for secure terminals (e.g., terminals that are locally attached to the host or connected to the host via secure leased lines), there is NO FINDING.

Fix Text: The Systems programmer and IAO will verify that USSTAB definitions are only used for secure terminals.

Only terminals that are locally attached to the host or connected to the host via secure leased lines located in a secured area. Only authorized personnel may enter the area where secure terminals are located.

USSTAB or LOGAPPL definitions are used to control logon from secure terminals. These terminals can log on directly to any VTAM application (e.g., TSO, CICS, etc.) of their choice and bypass Session Manager services. Secure terminals are usually locally attached to the host or connected to the host via a private LAN without access to an external network. Only authorized personnel may enter the area where secure terminals are located.

CCI: CCI-001499

Group ID (Vulid): V-6956

Group Title: ZVTM0018

Rule ID: SV-7359r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZVTM0018](#)

Rule Title: The System datasets used to support the VTAM network are not properly secured.

Vulnerability Discussion: VTAM options and definitions are used to define VTAM operational capabilities. They must be strictly controlled. Unauthorized users could override or change start options or network definitions. Failure to properly control VTAM resources could potentially compromise the network operations.

Responsibility: Systems Programmer

IAControls: N/A

Check Content:

- a) Create a list of data set names containing all VTAM start options, configuration lists, network resource definitions, commands, procedures, exit routines, all SMP/E TLIBs, and all SMP/E DLIBs used for installation and in development/production VTAM environments.

Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(VTAMRPT)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZVTM0018)

- b) Ensure that ACF2 data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

- c) If (b) above is true, there is NO FINDING.

- d) If (b) above is untrue, this is a FINDING.

Fix Text: The IOA will ensure that ACF2 data set rules for all VTAM system data sets restrict access to only network systems programming staff.

Ensure that ACF2 data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Example:

```
$KEY(SYS1)
VTAM-- UID(syspautd) R(A) W(L) A(L) E(A)
```

```
$KEY(S3V)
$PREFIX(SYS3)
VTAM-- UID(syspautd) R(A) W(L) A(L) E(A)
```

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-3897

Group Title: ZWAS0010

Rule ID: SV-3897r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0010](#)

Rule Title: MVS data sets for the WebSphere Application Server are not protected in accordance with the proper security requirements.

Vulnerability Discussion: MVS data sets provide the configuration, operational, and executable properties of the WebSphere Application Server (WAS) environment. Failure to properly protect these data sets may lead to unauthorized access. This exposure could compromise the integrity and availability of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(HTTPRPT)
- SENSITVE.RPT(WASRPT)

b) Ensure the following data set controls are in effect for WAS:

___ The ACP data set rules restrict UPDATE and ALTER access to HTTP product data sets (i.e., SYS1.IMW.AIMW** and SYS1.IMW.SIMW**) is restricted to systems programming personnel.

NOTE: If the HTTP server is not used with WAS, this check can be ignored.

___ The ACP data set rules restrict UPDATE and ALTER access to WAS product data sets and associated product data sets are restricted to systems programming personnel.

SYS*.EJS.V3500108.** (WebSphere 3.5)

SYS*.WAS.V401.** (WebSphere 4.0.1)

SYS*.OE.** (Java)

SYS*.JAVA** (Java)

SYS*.DB2.V710107.** (DB2)

SYS*.GLD.** (LDAP)

SYS1.LE.** (Language Environment)

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: The IAO will ensure that WebSphere server data sets restrict UPDATE and/or ALTER access to systems programming personnel.

Ensure the following data set controls are in effect for WAS:

1) UPDATE and ALTER access to HTTP product data sets (i.e., SYS1.IMW.AIMW** and SYS1.IMW.SIMW**) are restricted to systems programming personnel.

NOTE: If the HTTP server is not used with WAS, this check can be ignored.

2) UPDATE and ALTER access to WAS product data sets and associated product data sets are restricted to systems programming personnel.

SYS*.EJS.V3500108.** (WebSphere 3.5)

SYS*.WAS.V401.** (WebSphere 4.0.1)

SYS*.OE.** (Java)

SYS*.JAVA** (Java)

SYS*.DB2.V710107.** (DB2)

SYS*.GLD.** (LDAP)

SYS1.LE.** (Language Environment)

CCI: CCI-000213

Group ID (Vulid): V-3898

Group Title: ZWAS0020

Rule ID: SV-3898r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0020](#)

Rule Title: HFS objects for the WebSphere Application Server are not protected in accordance with the proper security requirements.

Vulnerability Discussion: HFS directories and files provide the configuration, operational, and executable properties of the WebSphere Application Server (WAS) environment. Many of these objects are responsible for the security implementation of WAS. Failure to properly protect these directories and files may lead to unauthorized access. This exposure could potentially compromise the integrity and availability of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following reports produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(IHSHFSOB)
- USSCMDS.RPT(WASHFSOB)

For each IBM HTTP server, supply the following information: (PDS member name - IHSACCTS)

- Web server ID defined to the ACP
- Web server administration group defined to the ACP
- Web server standard HFS directory

b) The following notes apply to the requirements specified in the HFS Permission Bits table in the z/OS STIG Addendum:

- If an owner field indicates UID(0) user, any system ID with a UID(0) specification is acceptable.
- Where an owner field indicates webserv1, the ID of the web server is intended.
- Where a group field indicates webadmgl, the ID of a local web server administration group is intended. IMWEB is not a valid local group.
- The site is free to set the permission and audit bit settings to be more restrictive than the documented values.

Ensure the HFS permission bits, user audit bits, owner, and group for each directory and file match the specified settings listed in the HFS Permission Bits table in the z/OS STIG Addendum. Currently the guidance requires the permissions on these files to be 640, where the group is the SA or web manager account that controls the web service. However the group permission only allows READ access making it impossible to update files unless using a UID(0) account. There appears to be a conflict with this requirement. Proposed updates include changing permissions from 640 to 460. The owner will be the web server user account and the group will be the web server administrator group.

Verification of these proposed changes needs to be performed. Until this occurs, compliance of the WAS configuration and property files cannot be reviewed. An entry for was.conf file settings needs to be added. Settings for the WebSphere properties and bin directories may be desirable.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rx | (least restrictive) |
| 6 | rw- | |
| 3 | -wx | |
| 2 | -w- | |
| 5 | r-x | |
| 4 | r-- | |
| 1 | --x | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

- f log for failed access attempts
- a log for failed and successful access
- no auditing

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Review the UNIX permission bits, user audit bits, and ownership settings on the HFS directories and files for the products required to support the WAS environment.

Ensure the HFS permission bits, user audit bits, owner, and group for each directory and file match the specified settings listed in the HFS Permissions Bits table located in the zOS STIG Addendum.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-3899

Group Title: ZWAS0030

Rule ID: SV-7265r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0030](#)

Rule Title: The CBIND Resource Class for the WebSphere Application Server is not configured in accordance with security requirements.

Vulnerability Discussion: SAF resources provide the ability to control access to functions and services of the WebSphere Application Server (WAS) environment. Many of these resources provide operational and administrative support for WAS. Failure to properly protect these resources may lead to unauthorized access. This exposure could compromise the integrity and availability of application services and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)

- SENSITIVE.RPT(CBIND)

b) Ensure the following items are in effect for CBIND resource protection:

2) The CLASMAP record defines the CBIND resource class.

3) The CB.BIND.server_name resource is defined to the CBIND resource class with a default access of PREVENT.

4) Access to the CB.BIND.server_name resource is restricted to WAS server (STC) logonids and systems management logonids (e.g., WebSphere administrator ID).

c) If all items in (b) are true, there is NO FINDING.

e) If any item in (b) is untrue, this is a FINDING.

Fix Text: There are two profiles to create when using the CBIND class. They are the CB.BIND.server_name profile, which controls whether a local or remote client can access servers. The CB.BIND is mandatory for the first two qualifiers for the profile; the third qualifier is the server name. Also, there is the CB.server_name profile that controls whether a client can use components in a server; again these definitions are mandatory.

Ensure the following items are in effect for CBIND resource protection:

1) The CBIND resource class is active.

2) The CB.BIND.server_name resource is defined to the CBIND resource class with a UACC(NONE).

3) Access to the CB.BIND.server_name resource is restricted to WAS server (STC) userids and systems management userids (e.g., WebSphere administrator ID).

The following command provide sample definitions and permissions for this CBIND resource:

```
SETR CLASSACT(CBIND)
SETR GENERIC(CBIND)
SETR RACL(CBIND)
```

```
RDEFINE CBIND cb.bind.<servername> UACC(none) owner(admin) audit(all(read)) data('IAW SRR PDI ZWAS0030')
```

```
Permit cb.bind.<servername> CLASS(CBIND) ID(<wscfg1>) ACCESS(CONTROL)
```

Note: "wscfg1" is a RACF group that contains the Websphere Application Server STCs and maintenance userids.

CCI: CCI-000213

Group ID (Vulid): V-3900

Group Title: ZWAS0040

Rule ID: SV-3900r2_rule

Severity: CAT I

Rule Version (STIG-ID): [ZWAS0040](#)

Rule Title: Vendor-supplied user accounts for the WebSphere Application Server are defined to the ACP.

Vulnerability Discussion: Vendor-supplied user accounts are defined to the ACP with factory-set passwords during the installation of the WebSphere Application Server (WAS). These user accounts are common to all WAS environments and have access to restricted resources and functions. Failure to delete vendor-supplied user accounts from the ACP may lead to unauthorized access. This exposure could compromise the integrity and availability of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

a) Refer to the following report produced by the ACP Data Collection:

ACF2

- ACF2CMDS.RPT(LOGONIDS)

RACF

- RACFCMDS.RPT(LISTUSER)

TSS

- TSSCMDS.RPT(@ACIDS)

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZWAS0040)

b) If the CBADMIN user account is not defined to the ACP, there is NO FINDING.

c) If the CBADMIN user account is defined to ACP and the password has NOT been changed from the vendor default of CBADMIN, this is a FINDING with a severity code of CAT I.

d) If the CBADMIN user account is defined to the ACP and the password has been changed from the vendor default of CBADMIN, this is a FINDING with a severity code of CAT II.

Fix Text: The IAO will ensure that the CBADMIN user account is removed or not defined to the ACP.

CCI: CCI-001762

Group ID (Vulid): V-3901

Group Title: ZWAS0050

Rule ID: SV-3901r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0050](#)

Rule Title: The WebSphere Application Server plug-in is not specified in accordance with the proper security requirements.

Vulnerability Discussion: Requests processed by the WebSphere Application Server (WAS) are dependent on directives configured in the HTTP server httpd.conf file. These directives specify critical files containing the WAS plug-in and WAS configuration. These files provide the operational and security characteristics of WAS. Failure to properly configure WAS-related directives could lead to undesirable operations and degraded security. This exposure may compromise the availability and integrity of applications and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following item gathered from the IBM HTTP Server Worksheet in the Preliminary Information Worksheets:

1. DOC(IHSPROCS)

b) Review the HTTP server JCL procedure to determine the httpd.conf file to review.

c) Ensure that all WAS-related directives are configured using the ServerInit, Service, and ServerTerm statements as outlined below.

The following path entries were added to the /etc/httpd.conf file for WebSphere 3.5:

```

ServerInit _/usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit
/usr/lpp/WebSphere/etc/WebSphere/AppServer/properties/was.conf
Service _/webapp/examples/* usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.jhtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.shtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/servlet/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.jsp /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
ServerTerm _/usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit

```

The following path entries are added to the /etc/httpd.conf file for WebSphere 4.0.1:

```

ServerInit - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:init_exit
Service - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:service_exit
ServerTerm - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:term_exit

```

NOTE:_The /etc/WebSphere clause for ServerInit matches the directory name above where the site customization was.conf file was established.

. Specific items to review include proper path, was.conf, and plug-in settings.

d) If all WAS-related directives are configured properly, there is NO FINDING.

e) If any WAS-related directive is not configured properly, this is a FINDING.

Fix Text: The IAO will ensure that the WebSphere Application Server directives in the httpd.conf file are configured as outlined below.

Ensure that all WAS-related directives are configured using the ServerInit, Service, and ServerTerm statements as outlined below.

The following path entries were added to the /etc/httpd.conf file for WebSphere 3.5:

```

ServerInit /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit /usr/lpp/WebSphere/etc/WebSphere/AppServer/properties/was.conf
Service /webapp/examples/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /*.jhtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /*.shtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /servlet/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /*.jsp /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit ServerTerm /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit

```

The following path entries are added to the /etc/httpd.conf file for WebSphere 4.0.1:

```

ServerInit -/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:init_exit

```


Service - /usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:service_exit
ServerTerm - /usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:term_exit

NOTE: The /etc/WebSphere clause for ServerInit matches the directory name above where the site customization was.conf file was established. Specific items to review include proper path, was.conf, and plug-in settings.

CCI: CCI-000068

CCI: CCI-000382

CCI: CCI-001762

Group ID (Vulid): V-6958

Group Title: ZWMQ0011

Rule ID: SV-7259r4_rule

Severity: CAT I

Rule Version (STIG-ID): [ZWMQ0011](#)

Rule Title: WebSphere MQ channel security must be implemented in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ Channel security can be configured to provide authentication, message privacy, and message integrity between queue managers. Secure Sockets Layer (SSL) uses encryption techniques, digital signatures and digital certificates to provide message privacy, message integrity and mutual authentication between clients and servers.

Failure to properly secure a WebSphere MQ channel may lead to unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of some system services, applications, and customer data.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECNK-1, ECNK-2

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

Below is a sample of the WebSphere MQ channel definition needed to remediate this STIG.

b) For each WebSphere MQ channel configured to communicate with servers using WebSphere MQ, review the ssid report(s) and perform the following steps:

1. Verify that each WebSphere MQ channel is using SSL by checking for the SSLCIPH parameter, which specifies a cipher specification:

```
ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
```

(Both ends of the channel must specify the same cipher specification.)

2. Repeat these steps for each queue manager ssid identified.

c) For each queue manager ssid identified, if the SSLCIPH parameter, on both sides of each WebSphere MQ channel, specifies the above in b. there is NO FINDING.

d) If the communication lines are controlled by a VPN and are not available in the clear at any point outside the enclave, than this is acceptable and can override the requirement to use SSL. If this is true, there is NO FINDING.

e) For each queue manager ssid identified , if either side of each WebSphere MQ channel specifies a cipher specification other than specified in b , this is a FINDING unless the communication lines are controlled by a VPN and traffic is not available in the clear at any point outside of the enclave.

For each queue manager ssid identified, if either side of each WebSphere MQ channel specifies a cipher specification other than DES or DES3, and the communication lines are not controlled by a VPN, this is a FINDING.

Fix Text: The system programmer and the IAO will review the WebSphere MQ Screen interface invoked by the REXX CSQOREXX. Reviewing the channel s SSLCIPH setting.

Display the channel properties and look for the "SSL Cipher Specification" value.

Ensure that a FIPS 140-2 compliant value is shown.

ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256

Note that both ends of the channel must specify the same cipher specification.

Repeat these steps for each queue manager ssid identified.

CCI: CCI-000068

CCI: CCI-002421

CCI: CCI-002423

CCI: CCI-002450

Group ID (Valid): V-6980

Group Title: ZWMQ0012

Rule ID: SV-7283r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0012](#)

Rule Title: WebSphere MQ channel security is not implemented in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ channel security can be configured to provide authentication, message privacy, and message integrity between queue managers. WebSphere MQ channels use SSL encryption techniques, digital signatures and digital certificates to provide message privacy, message integrity and mutual authentication between clients and servers.

Failure to properly secure a WebSphere MQ channel may lead to unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of some system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier). To determine which Release of WebSphere MQ, review ssid reports for message CSQU0001.

Collect the following Information for Websphere MQ queue manager

- If a WebSphere MQ queue manager communicates with a MQSeries queue manager, provide the WebSphere MQ queue manager and channel names used to connect with MQSeries.
- If any WebSphere MQ channels are used to communicate within the enclave, provide a list of channels and provide documentation regarding the sensitivity of the information on the channel.

b) Review the ssid report(s) and perform the following steps:

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following ACF2 command, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtained from the above action:

LIST ssidCHIN PROFILE(CERTDATA, KEYRING)

The output will contain information on the CERTDATA and KEYRING records for the user. Find the CERTDATA entry that has a Key ring name field with sslkeyring-id. Review the ISSUERDN field for this CERTDATA record for the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
 OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.
- c) If the all of the items in (b) above are true, there is NO FINDING.
- d) If any of the items in (b) above are untrue, this is a FINDING.

Check Content:

- a) Refer to the following report produced by the z/OS Data Collection:
- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier). To determine which Release of WebSphere MQ, review ssid reports for message CSQU000I.

Collect the following Information for Websphere MQ queue manager

- If a WebSphere MQ queue manager communicates with a MQSeries queue manager, provide the WebSphere MQ queue manager and channel names used to connect with MQSeries.
 - If any WebSphere MQ channels are used to communicate within the enclave, provide a list of channels and provide documentation regarding the sensitivity of the information on the channel.
- b) Review the ssid report(s) and perform the following steps:
 - 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
 - 2) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is

identified. i.e. SSLKEYR(sslkeyring-id)

3) Issue the following RACF commands, where ssidCHIN is the logonid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtained from the above action:

RACDCERT ID(ssidCHIN) LISTRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

The output will contain columns for Certificate Label Name and Cert Owner. Find the Cert Owner of ID(ssidCHIN). Use the Certificate Label Name for ID(ssidCHIN) in the following command:

RACDCERT ID(ssidCHIN) LIST(LABEL(Certificate Label Name))

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US

OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.
- c) If the all of the items in (b) above are true, there is NO FINDING.
- d) If any of the items in (b) above are untrue, this is a FINDING.

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier). To determine which Release of WebSphere MQ, review ssid reports for message CSQU000I.

Collect the following Information for Websphere MQ queue manager

- If a WebSphere MQ queue manager communicates with a MQSeries queue manager, provide the WebSphere MQ queue manager and channel names used to connect with MQSeries.
- If any WebSphere MQ channels are used to communicate within the enclave, provide a list of channels and provide documentation regarding the sensitivity of the information on the channel.

b) Review the ssid report(s) and perform the following steps:

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following TSS commands, where ssidCHIN is the Acid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtained from the above action:

TSS LIST(ssidCHIN) KEYRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

In the output find the DIGICERT field for ACID(ssidCHIN). Use this DIGICERT in the following command:

TSS LIST(ssidCHIN) DIGICERT(digicert)

NOTE: The digicert is case sensitive.

Review the ISSUER DISTINGUISHED NAME field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.
- c) If the all of the items in (b) above are true, there is NO FINDING.
- d) If any of the items in (b) above are untrue, this is a FINDING.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following RACF commands, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtain from the

above action:

RACDCERT ID(ssidCHIN) LISTRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

The output will contain columns for Certificate Label Name and Cert Owner. Find the Cert Owner of ID(ssidCHIN). Use the Certificate Label Name for ID(ssidCHIN) in the following command:

RACDCERT ID(ssidCHIN) LIST(LABEL(Certificate Label Name))

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US

OU=ECA.O=U.S. Government.C=US

4) Repeat these steps for each queue manager ssid identified.

To implement the requirements stated above, the following two items are provided which attempt to assist with (1) Technical "how to" information and (2) A DISA Point of contact for obtaining SSL certificates for CSD WebSphere MQ channels:

1. Review the information available on setting up SSL, Keyrings, and Digital Certificates in the RACF Security Administrator's Guide as well as the WebSphere MQ Security manual. Also review the information contained in the documentation provided as part of the install package from the DISA SSO Resource Management Factory (formerly Software Factory).
2. For information on obtaining an SSL certificate in the DISA CSD environment, send email inquiry to disaraoperations@disa.mil for more info.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following ACF2 command, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtain from the above action:

LIST ssidCHIN PROFILE(CERTDATA, KEYRING)

The output will contain information on the CERTDATA and KEYRING records for the user. Find the CERTDATA entry that has a Key ring name field with sslkeyring-id. Review the ISSUERDN field for this CERTDATA record for the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US

4) Repeat these steps for each queue manager ssid identified.

To implement the requirements stated above, the following two items are provided which attempt to assist with (1) Technical "how to" information and (2) A DISA Point of contact for obtaining SSL certificates for CSD WebSphere MQ channels:

1. Review the information available on setting up SSL, Keyrings, and Digital Certificates in the CA-ACF2 Security for z/OS Administrators Guide as well as the WebSphere MQ Security manual. Also review the information contained in the documentation provided as part of the install package from the DISA SSO Resource Management Factory (formerly Software Factory).

2. For information on obtaining an SSL certificate in the DISA CSD environment, send email inquiry to disaraoperations@disa.mil for more info.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following TSS commands, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtain from the above action:

TSS LIST(ssidCHIN) KEYRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

In the output find the DIGICERT field for ACID(ssidCHIN). Use this DIGICERT in the following command:

```
TSS LIST(ssidCHIN) DIGICERT(digicert)
```

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US

OU=ECA.O=U.S. Government.C=US

4) Repeat these steps for each queue manager ssid identified.

To implement the requirements stated above, the following two items are provided which attempt to assist with (1) Technical "how to" information and (2) A DISA Point of contact for obtaining SSL certificates for CSD WebSphere MQ channels:

1. Review the information available on setting up SSL, Keyrings, and Digital Certificates in the CA TSS Cookbook regarding usage of the TSS commands to administer PKI Certificates as well as the WebSphere MQ Security manual. Also review the information contained in the documentation provided as part of the install package from the DISA SSO Resource Management Factory (formerly Software Factory).

2. For information on obtaining an SSL certificate in the DISA CSD environment, send email inquiry to disaraoperations@disa.mil for more info.

CCI: CCI-002470

Group ID (Vulid): V-31561

Group Title: ZWMQ0014

Rule ID: SV-41848r5_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0014](#)

Rule Title: Production WebSphere MQ Remotes must utilize Certified Name Filters (CNF)

Vulnerability Discussion: IBM Websphere MQ can use a user ID associated with an ACP certificate as a channel user ID. When an entity at one end of an SSL channel receives a certificate from a remote connection, the entity asks The ACP if there is a user ID associated with that certificate. The entity uses that user ID

as the channel user ID. If there is no user ID associated with the certificate, the entity uses the user ID under which the channel initiator is running. Without a validly defined Certificate Name Filter for the entity IBM Websphere MQ will set the channel user ID to the default.

Responsibility: N/A

IAControls: N/A

Check Content:

Validate that the list of all Production WebSphere MQ Remotes exist, and contains approved Certified Name Filters and associated USERIDS.

If the filter(s) is (are) defined, accurate and has been approved by Vulnerability ICER0030 and the associated USERID(s) is only granted need to know permissions and authority to resources and commands, this is not a finding.

If there is no Certificate Name Filter for WebSphere MQ Remotes this is a Finding.

Note: Improper use of CNF filters for MQ Series will result in the following Message ID.

CSQX632I found in the following example:

CSQX632I csect-name SSL certificate has no
associated user ID, remote channel
channel-name channel initiator user ID
used

Fix Text: The responsible MQ System programmer(s) shall create and maintain a spread sheet that contains a list of all Production WebSphere MQ Remotes, associated individual USERIDs with corresponding valid Certified Name Filters (CNF). This documentation will be reviewed and validated annually by responsible MQ System programmer(s) and forwarded for approval by the ISSM.

The ISSO will define the associated USERIDs, the CNF, and grant the minimal need to know access, by granting only the required resources and Commands for each USERID in the ACP. See IBM WebSphere MQ Security manual for details on defining CNF for WebSphere MQ.

Generic access shall not be granted such as resource permission at the SSID. MQ resource level.

CCI: CCI-000366

CCI: CCI-001133

Group ID (Vulid): V-3903

Group Title: ZWMQ0020

Rule ID: SV-3903r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0020](#)

Rule Title: User timeout parameter values for WebSphere MQ queue managers are not specified in accordance with security requirements.

Vulnerability Discussion: Users signed on to a WebSphere MQ queue manager could leave their terminals unattended for long periods of time. This may allow unauthorized individuals to gain access to WebSphere MQ resources and application data. This exposure could compromise the availability, integrity, and confidentiality of some system services and application data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

b) Review messages CSQH015I and CSQH016I:

12.36.22 STC01960 CSQH015I !MQ19 Security timeout = 15 minutes

12.36.22 STC01960 CSQH016I !MQ19 Security interval = 5 minutes

The Z/OS STIG standard value for interval is: INTERVAL(5).

The Z/OS STIG standard value for timeout is: TIMEOUT(15)

c) If the timeout value equals 15 minutes, there is NO FINDING.

If the interval value equals 5 minutes, there is NO FINDING.

d) If the timeout value does not equal 15 minutes, this is a FINDING

If the interval value is not equal to 5 minutes, this is a FINDING

Repeat steps (a) thru (d) for each queue manager ssid.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

Fix Text: Review the WebSphere MQ System Setup Guide and the information on the ALTER SECURITY command in the WebSphere MQ Script (MQSC) Command Reference.

Ensure the values for the TIMEOUT and INTERVAL parameters are specified in accordance with security requirements.

CCI: CCI-001133

Group ID (Vulid): V-3904

Group Title: ZWMQ0030

Rule ID: SV-7526r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0030](#)

Rule Title: WebSphere MQ started tasks are not defined in accordance with the proper security requirements.

Vulnerability Discussion: Started tasks are used to execute WebSphere MQ queue manager services. Improperly defined WebSphere MQ started tasks may result in inappropriate access to application resources and the loss of accountability. This exposure could compromise the availability of some system services and application data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following reports produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(LOGONIDS)
- ACF2CMDS.RPT(ATTSTC)

Provide a list of all WebSphere MQ Subsystem Ids (Queue managers) and Release levels.

b) Review WebSphere MQ started tasks and ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

ssidMSTR is the name of a queue manager STC.

ssidCHIN is the name of a distributed queuing (a.k.a., channel initiator) STC.

- 1) Each ssidMSTR and ssidCHIN started task is associated with a unique logonid.
 - 2) Each ssidMSTR and ssidCHIN STC logonid has the attributes of STC, MUSASS, and NOSMC.
- c) If both of the items in (b) are true, there is NO FINDING.
- d) If either item in (b) is untrue, this is a FINDING.

Fix Text: Each queue manager started task procedure xxxxMSTR and distributed queuing started task procedure xxxxCHIN will have a matching profile defined to the STARTED resource class. Create a corresponding userid for each started task. The STC userids will be defined as PROTECTED userids. Queue manager and channel initiator started tasks will not be defined with the TRUSTED attribute.

The following sample contains commands to properly define the required Started Procs:

Note that this example uses "qmq1" as the value for ssid.

```
AU qmq1mstr NAME('STC, MQSERIES') NOPASS DFLTGRP(STC) OWNER(STC) DATA('MQSERIES QUEUE MANAGER PROC')
```

```
AU qmq1chin NAME('STC, MQSERIES') NOPASS DFLTGRP(STC) OWNER(STC) DATA('MQSERIES DISTRIBUTED QUEUING CHANNEL INIT PROC')
```

```
RDEF STARTED qmq1mstr.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MAP qmq1mstr PROC TO qmq1mstr USERID')  
STDATA(USER(=MEMBER) GROUP(STC) TRACE(YES))
```

```
RDEF STARTED qmq1chin.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MAP qmq1mstr PROC TO qmq1chin USERID')
STDATA(USER(=MEMBER) GROUP(STC) TRACE(YES))
```

```
SETR RACL(STARTED) REFRESH
```

CCI: CCI-000764

Group ID (Vulid): V-3905

Group Title: ZWMQ0040

Rule ID: SV-3905r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0040](#)

Rule Title: WebSphere MQ all update and alter access to MQSeries/WebSphere MQ product and system data sets are not properly restricted

Vulnerability Discussion: MVS data sets provide the configuration, operational, and executable properties of WebSphere MQ. Some data sets are responsible for the security implementation of WebSphere MQ. Failure to properly protect these data sets may lead to unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the ACP Data Collection:

- SENSITVE.RPT(MQSRPT)

b) Ensure ACP data sets rules for MQSeries/WebSphere MQ system data sets (e.g., SYS2.MQM.) restrict access as follows:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

____ READ access to data sets referenced by the following DDnames is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel. All access to these data sets is logged.

| DDname | Procedure | Description |
|---------|-----------|------------------|
| CSQINP1 | ssidMSTR | Input parameters |
| CSQINP2 | ssidMSTR | Input parameters |

CSQXLIB ssidCHIN User exit library

NOTE: WRITE/UPDATE and/or ALLOCATE/ALTER access to these data sets is restricted to MQSeries/WebSphere MQ administrators and systems programming personnel.

____ WRITE/UPDATE and/or ALLOCATE/ALTER access to data sets referenced by the following DDnames is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and systems programming personnel. All WRITE and ALLOCATE access to these data sets is logged.

| DDname | Procedure | Description |
|------------|-----------|---------------------|
| CSQPxxxx | ssidMSTR | Page data sets |
| BSDSx | ssidMSTR | Bootstrap data sets |
| CSQOUTx | ssidMSTR | SYSOUT data sets |
| CSQSNAP | ssidMSTR | DUMP data set |
| (See note) | ssidMSTR | Log data sets |

NOTE: To determine the log data set names, review the JESMSGLG file of the ssidMSTR active task(s). Find CSQJ001I messages to obtain DSNs.

____ ALLOCATE/ALTER access to archive data sets is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel. All ALLOCATE/ALTER access to these data sets is logged.

NOTE: To determine the archive data sets names, review the JESMSGLG file of the ssidMSTR active task(s). Find the CSQY122I message to obtain the ARCPRF1 and ARCPRF2 DSN HLQs.

____ Except for the specific data set requirements just mentioned, WRITE/UPDATE and/or ALLOCATE/ALTER access to all other MQSeries/WebSphere MQ system data sets is restricted to the MQSeries/WebSphere MQ administrator and system programming personnel.

c) If all the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: The systems programmer will have the IAO ensure that all update and alter access to MQSeries/WebSphere MQ product and system data sets are restricted to WebSphere MQ administrators, systems programmers, and MQSeries/WebSphere MQ started tasks.

The installation requires that the following data sets be APF authorized.

hlqual.SCSQAUTH
hlqual.SCSQLINK
hlqual.SCSQANLx
hlqual.SCSQSNL

hlqual.SCSQMVR1
hlqual.SCSQMVR2

- (2) Read access to data sets referenced by the CSQINP1, CSQINP2, and CSQXLIB DDs in the queue manager s procedure will be restricted to the queue manager userid, WebSphere MQ administrator, and systems programming personnel. Log all access to these data sets.
- (3) Write and allocate access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager s procedure will be restricted to the queue manager userid, WebSphere MQ administrator, and systems programming personnel. Log all write and allocate access to these data sets.
- (5) Allocate access to all archive data sets in the queue manager s procedure will be restricted to the queue manager userid, WebSphere MQ administrator, and systems programming personnel. Log all allocate access to these data sets.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-6959

Group Title: ZWMQ0049

Rule ID: SV-7534r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0049](#)

Rule Title: WebSphere MQ resource classes are not properly activated for security checking by the ACP.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to ensure the classes have been made ACTIVE under RACF will prevent RACF from enforcing security rules. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)

Ensure the System Authorization Facility Definition (SAFDEF) include an entry for WebSphere MQ as follows:

```
INSERT SAFDEF.MQS ID(MQS) FUNCRET(8) RETCODE(4) MODE(IGNORE)
RACROUTE(REQUEST=EXTRACT,CLASS=MQADMIN) REP
```

Ensure the Internal CLASMAP Definitions include the following entries:

```
INSERT CLASMAP.MQADMIN RESOURCE(MQADMIN) RSRCTYPE(MQA) ENTITYLN(62)
INSERT CLASMAP.MQCMDS RESOURCE(MQCMDS) RSRCTYPE(MQC) ENTITYLN(22)
INSERT CLASMAP.MQCONN RESOURCE(MQCONN) RSRCTYPE(MQK) ENTITYLN(10)
INSERT CLASMAP.MQNLIST RESOURCE(MQNLIST) RSRCTYPE(MQN) ENTITYLN(53)
INSERT CLASMAP.MQPROC RESOURCE(MQPROC) RSRCTYPE(MQP) ENTITYLN(53)
INSERT CLASMAP.MQQUEUE RESOURCE(MQQUEUE) RSRCTYPE(MQQ) ENTITYLN(53)
```

For V7.0.0 and above:

```
INSERT CLASMAP.MXADMIN RESOURCE(MXADMIN) RSRCTYPE(MXA) ENTITYLN(62)
INSERT CLASMAP.MXNLIST RESOURCE(MXNLIST) RSRCTYPE(MXN) ENTITYLN(53)
INSERT CLASMAP.MXPROC RESOURCE(MXPROC) RSRCTYPE(MXP) ENTITYLN(53)
INSERT CLASMAP.MXQUEUE RESOURCE(MXQUEUE) RSRCTYPE(MXQ) ENTITYLN(53)
INSERT CLASMAP.MXTOPIC RESOURCE(MXTOPIC) RSRCTYPE(MXT) ENTITYLN(246)
```

Fix Text: The IAO will ensure that all WebSphere MQ resources are active and properly defined.

Ensure the System Authorization Facility Definition (SAFDEF) include an entry for WebSphere MQ as follows:

```
INSERT SAFDEF.MQS ID(MQS) FUNCRET(8) RETCODE(4) MODE(IGNORE)
RACROUTE(REQUEST=EXTRACT,CLASS=MQADMIN) REP
```

Ensure the Internal CLASMAP Definitions include the following entries:

```
INSERT CLASMAP.MQADMIN RESOURCE(MQADMIN) RSRCTYPE(MQA) ENTITYLN(62)
INSERT CLASMAP.MQQUEUE RESOURCE(MQQUEUE) RSRCTYPE(MQQ) ENTITYLN(53)
INSERT CLASMAP.MQNLIST RESOURCE(MQNLIST) RSRCTYPE(MQN) ENTITYLN(53)
INSERT CLASMAP.MQCMDS RESOURCE(MQCMDS) RSRCTYPE(MQC) ENTITYLN(22)
INSERT CLASMAP.MQCONN RESOURCE(MQCONN) RSRCTYPE(MQK) ENTITYLN(10)
```

```
INSERT CLASMAP.MQPROC RESOURCE(MQPROC) RSRCTYPE(MQP) ENTITYLN(53)
```

For V7.0.0 and above:

```
INSERT CLASMAP.MXADMIN RESOURCE(MXADMIN) RSRCTYPE(MXA) ENTITYLN(62)
INSERT CLASMAP.MXNLIST RESOURCE(MXNLIST) RSRCTYPE(MXN) ENTITYLN(53)
INSERT CLASMAP.MXPROC RESOURCE(MXPROC) RSRCTYPE(MXP) ENTITYLN(53)
INSERT CLASMAP.MXQUEUE RESOURCE(MXQUEUE) RSRCTYPE(MXQ) ENTITYLN(53)
INSERT CLASMAP.MXTOPIC RESOURCE(MXTOPIC) RSRCTYPE(MXT) ENTITYLN(246)
```

CCI: CCI-000213

CCI: CCI-002358

Group ID (Vulid): V-6960

Group Title: ZWMQ0051

Rule ID: SV-7538r2_rule

Severity: CAT I

Rule Version (STIG-ID): [ZWMQ0051](#)

Rule Title: WebSphere MQ "switch" profiles are improperly defined to the MQADMIN class.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
```

```
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

b) Review the Security switches. If all of the following switches specify ON, there is NO FINDING.

SUBSYSTEM CONNECTION COMMAND CONTEXT ALTERNATE USER
PROCESS NAMELIST QUEUE COMMAND RESOURCES

For example:

```
10.05.01 STC01960 CSQH030I !MQ19 Security switches ...
10.05.01 STC01960 CSQH034I !MQ19 SUBSYSTEM: ON,
10.05.01 STC01960 CSQH031I !MQ19 CONNECTION: ON,
10.05.01 STC01960 CSQH034I !MQ19 COMMAND: ON,
10.05.01 STC01960 CSQH031I !MQ19 CONTEXT: ON,
10.05.01 STC01960 CSQH034I !MQ19 ALTERNATE USER: ON,
10.05.01 STC01960 CSQH034I !MQ19 PROCESS: ON,
10.05.01 STC01960 CSQH034I !MQ19 NAMELIST: ON,
10.05.01 STC01960 CSQH034I !MQ19 QUEUE: ON,
10.05.01 STC01960 CSQH031I !MQ19 COMMAND RESOURCES: ON,
```

c) If the SUBSYSTEM switch is OFF, this is a FINDING with a severity of Category I.

d) If any of the other above switches specify OFF (other than the exception mentioned below), this is a FINDING, downgrade the severity to a Category II.

e) If the COMMAND RESOURCE Security switch specifies OFF, there is NO FINDING.

NOTE: At the discretion of the IAO, COMMAND RESOURCE Security switch may specify OFF, by defining ssid.NO.CMD.RESC.CHECKS in the MQADMIN resource class.

Fix Text: Switch profiles are special MQSeries/WebSphere MQ profiles that are used to turn on/off security checking for a type of resource. Due to the security exposure this creates, no profiles with the first two qualifiers of ssid.NO will be defined to the MQADMIN class, with one exception. Due to the fact that (1) all sensitive MQSeries/WebSphere MQ commands are restricted to queue managers, channel initiators, and designated systems personnel, and (2) no command resource checking is performed on DISPLAY commands, at the discretion of the IAO a ssid.NO.CMD.RESC.CHECKS switch profile may be defined to the MQADMIN class.

1. Identify if any switch profiles exist using the sample search command:

```
SR CLASS(MQADMIN) NOMASK FILTER(*.NO.**)
```

2. Use the "RDEL MQADMIN <SwitchProfileName>" to remove the profile and follow up with a "SETR RACL(MQADMIN) REF"

3. An additional refresh to an active WebSphere MQ Que Manager may be required. A sample is show below using the value QMD1 as the Que Manager name.

From the Console:

```
>QMD1 REFRESH SECURITY(*)
```

CCI: CCI-000213

Group ID (Vulid): V-6962

Group Title: ZWMQ0052

Rule ID: SV-7541r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0052](#)

Rule Title: WebSphere MQ MQCONN Class (Connection) resource definitions are not protected in accordance with security.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and

namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- SENSITVE.RPT(MQCONN)
- ACF2CMDS.RPT(RESOURCE) Alternate report

b) Review the following connection resources defined to TYPE(MQK) (i.e., MQCONN resource class):

Resource Authorized Users
ssid.BATCH TSO and batch job userids
ssid.CICS CICS region userids
ssid.IMS IMS region userids
ssid.CHIN Channel initiator userids

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

c) For all connection resources defined to TYPE(MQK), ensure the following items are in effect:

- 1) Access authorization to these connections restricts access to the appropriate users as indicated in (b).
- 2) All access FAILUREs are logged.

d) If both of the items in (c) are true, there is NO FINDING.

e) If either item in (c) is untrue, this is a FINDING.

Fix Text: Review the following connection resources defined to the MQCONN resource class:

| Resource | Authorized Users |
|------------|---------------------------|
| ssid.BATCH | TSO and batch job userids |
| ssid.CICS | CICS region userids |
| ssid.IMS | IMS region userids |
| ssid.CHIN | Channel initiator userids |

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

c) For all connection resources defined to the MQCONN resource class, ensure the following items are in effect:

NOTE: If you do not have a resource profile defined for a particular security check, and a user issues a request that would involve making that check, MQSeries/WebSphere MQ denies access.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization to these connections restricts access to the appropriate users as indicated in (b).
- 3) All access is logged, e.g., ALL(READ).

A set of sample commands are provided below to implement the minimum profiles necessary for proper security. Note that the IMS and/or CICS profiles can be omitted if those products do not run on the target system.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
RDEF MQCONN ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCONN DENY-BY-DEFAULT PROFILE')

RDEF MQCONN <ssid>.BATCH UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0052')
PE <ssid>.BATCH CL(MQCONN) ID(<applicableTSO&batchUsers>)

RDEF MQCONN <ssid>.CICS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0052')
PE <ssid>.CICS CL(MQCONN) ID(<CICSRegionUserids>)

RDEF MQCONN <ssid>.IMS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0052')
PE <ssid>.IMS CL(MQCONN) ID(<IMSRegionUserids>)

RDEF MQCONN <ssid>.CHIN UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0052')
PE <ssid>.CHIN CL(MQCONN) ID(<WebsphereMQCHINUsrids>)
```

```
SETR RACL(MQCONN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6964

Group Title: ZWMQ0053

Rule ID: SV-7267r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0053](#)

Rule Title: WebSphere MQ dead letter and alias dead letter queues are not properly defined.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) Review the ssid report(s) and perform the following steps:

1) Find the DISPLAY QMGR DEADQ command to locate the start of the dead-letter queue information. Review the DEADQ parameter to obtain the name of the real dead-letter queue.

2) From the top of the report, find the QUEUE(dead-letter.queue.name) entry to locate the start of the real dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to the specified security requirements.

The standard values are:

GET(ENABLED)

PUT(ENABLED)

NOTE: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

3) From the top of the report, find the QUEUE(dead-letter.queue.name.PUT) entry to locate the start of the alias dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to those specified in the security requirements.

The standard values are:

GET(DISABLED)

PUT(ENABLED)

NOTE 1: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

NOTE 2: The TARGQ parameter value for the alias queue will be the real dead letter queue name.

NOTE 3: If an alias queue is not used in place of the dead-letter queue, then the ACP rules for the dead-letter queue must be coded to restrict unauthorized users and systems from reading the messages on the file.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: a) Refer to the following report produced by the z/OS Data Collection:

- MQSRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) Review the ssid report(s) and perform the following steps:

1) Find the DISPLAY QMGR DEADQ command to locate the start of the dead-letter queue information. Review the DEADQ parameter to obtain the name of the real dead-letter queue.

2) From the top of the report, find the QUEUE(dead-letter.queue.name) entry to locate the start of the real dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to the specified security requirements.

The standard values are:

GET(ENABLED)
PUT(ENABLED)

NOTE: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

3) From the top of the report, find the QUEUE(dead-letter.queue.name.PUT) entry to locate the start of the alias dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to those specified in the security requirements.

The standard values are:

GET(DISABLED)
PUT(ENABLED)

NOTE 1: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

NOTE 2: The TARGQ parameter value for the alias queue will be the real dead letter queue name.

NOTE 3: If an alias queue is not used in place of the dead-letter queue, then the ACP rules for the dead-letter queue must be coded to restrict unauthorized users and systems from reading the messages on the file.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-001762

Group ID (Vulid): V-6965

Group Title: ZWMQ0054

Rule ID: SV-7544r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0054](#)

Rule Title: WebSphere MQ MQQUEUE (Queue) resource profiles defined to the MQQUEUE class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- MQSRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) Review the ssid report(s) and perform the following steps:

1) Find the DISPLAY QMGR DEADQ command to locate the start of the dead-letter queue information. Review the DEADQ parameter to obtain the name of the real dead-letter queue.

2) From the top of the report, find the QUEUE(dead-letter.queue.name) entry to locate the start of the real dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to the specified security requirements.

The standard values are:

GET(ENABLED)

PUT(ENABLED)

NOTE: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

3) From the top of the report, find the QUEUE(dead-letter.queue.name.PUT) entry to locate the start of the alias dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to those specified in the security requirements.

The standard values are:

GET(DISABLED)

PUT(ENABLED)

NOTE 1: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

NOTE 2: The TARGQ parameter value for the alias queue will be the real dead letter queue name.

NOTE 3: If an alias queue is not used in place of the dead-letter queue, then the ACP rules for the dead-letter queue must be coded to restrict unauthorized users and systems from reading the messages on the file.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(MQQUEUE)

For all queue identified by the DISPLAY QUEUE(*) ALL command in the MQRPT(ssid). These queues will be prefixed by ssid to identify the resources to be protected. Ensure these queue resources are defined to the MQQUEUE or GMQUEUE resource classes, if the following guidance is true, this is not a finding.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) For message queues (i.e., ssid.queueName), access authorization restricts access to users requiring the ability to get messages from and put messages to message queues. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list. Decentralized MQ Administrators, non-DECC datacenter users; can have up to ALTER access to the user Message Queues.
- 3) For system queues (i.e., ssid.SYSTEM.queueName), access authorization restricts UPDATE and/or ALTER access to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, and CICS regions running WebSphere MQ applications.
- 4) For the following system queues ensure that UPDATE access is restricted to Auditors and Users that require access to review message queues.
ssid.SYSTEM.COMMAND.INPUT
ssid.SYSTEM.COMMAND.REPLY
ssid.SYSTEM.CSQOREXX.*
- 5) For the real dead-letter queue (to determine queue name refer to ZWMQ0053), ALTER access authorization restricts access to WebSphere MQ STCs, WebSphere MQ administrators, CICS regions running WebSphere MQ applications, and any automated application used for dead-letter queue maintenance.
- 6) For the alias dead-letter queue (to determine queue name refer to ZWMQ0053), UPDATE access authorization restricts access to users requiring the ability to put messages to the dead-letter queue. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

Fix Text: For all queue resources defined to the MQQUEUE or GMQUEUE resource classes, ensure the following items are in effect:

For all queue identified by the DISPLAY QUEUE(*) ALL command in the MQRPT(ssid). These queues will be prefixed by ssid to identify the resources to be protected. Ensure these queue resources are defined to the MQQUEUE or GMQUEUE resource classes, if the following guidance is true, this is not a finding.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) For message queues (i.e., ssid.queueName), access authorization restricts access to users requiring the ability to get messages from and put messages to message queues. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list. Decentralized MQ Administrators, non-DECC datacenter users; can have up to ALTER access to the user Message Queues.
- 3) For system queues (i.e., ssid.SYSTEM.queueName), access authorization restricts UPDATE and/or ALTER access to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, and CICS regions running WebSphere MQ applications.
- 4) For the following system queues ensure that UPDATE access is restricted to Auditors and Users that require access to review message queues.
ssid.SYSTEM.COMMAND.INPUT
ssid.SYSTEM.COMMAND.REPLY
ssid.SYSTEM.CSQOREXX.*
ssid.SYSTEM.CSQUTIL.*
- 5) For the real dead-letter queue (to determine queue name refer to ZWMQ0053), ALTER access authorization restricts access to WebSphere MQ STCs, WebSphere MQ administrators, CICS regions running WebSphere MQ applications, and any automated application used for dead-letter queue maintenance.
- 6) For the alias dead-letter queue (to determine queue name refer to ZWMQ0053), UPDATE access authorization restricts access to users requiring the ability to put messages to the dead-letter queue. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

Example:

```
RDEF MQQUEUE <ssid>.SYSTEM.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ)) DATA('REQUIRED FOR ZWMQ0054')  
PE <ssid>.SYSTEM.** CL(MQQUEUE) ID(<RestrictedUsersAsSpecifiedAbove>)
```

```
RDEF MQQUEUE <ssid>.<qname>.* UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ)) DATA('REQUIRED FOR ZWMQ0054')  
PE <ssid>.<qname> CL(MQQUEUE) ID(<AsSpecifiedAbove>)
```

```
RDEF MQQUEUE <ssid>.<RealDeadLetterQue>.* UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ)) DATA('REQUIRED FOR ZWMQ0054')  
PE <ssid>.<RealDeadLetterQue> CL(MQQUEUE) ID(<AsSpecifiedAbove>)
```

```
RDEF MQQUEUE <ssid>.<AliasDeadLetterQue>.* UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ)) DATA('REQUIRED FOR ZWMQ0054')  
PE <ssid>.<AliasDeadLetterQue> CL(MQQUEUE) ID(<AsSpecifiedAbove>)
```

```
SETR RACL(MQQUEUE) REF
```

CCI: CCI-000213

Group ID (Vulid): V-6966

Group Title: ZWMQ0055

Rule ID: SV-7546r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0055](#)

Rule Title: WebSphere MQ Process resource profiles defined in the MQPROC Class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ Process resources allow for the control of processes. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- SENSITIVE.RPT(MQPROC)
- ACF2CMDS.RPT(RESOURCE) Alternate report

b) For all process resources (i.e., ssid.processname) defined to TYPE(MQP) (i.e., MQPROC resource class), ensure access authorization restricts access to users requiring the ability to make process inquiries. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

c) If (b) is true, there is NO FINDING.

d) If (b) is untrue, this is a FINDING.

Fix Text: Process security validates userids authorized to issue MQSeries / WebSphere MQ inquiries on process definitions. A process definition object defines an application that is started in response to a trigger event on a queue manager. Process security will be active, and all profiles ssid.processname will be defined to the MQPROC class. Restrict read access to those userids requiring access to make process inquiries.

For all process resources (i.e., ssid.processname) defined to the MQPROC or GMQPROC resource classes, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to make process inquiries. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
RDEF MQPROC ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQPROC DENY-BY-DEFAULT PROFILE')

RDEF MQPROC <ssid>.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0055')
PE <ssid>.* CL(MQPROC) ID(<ApplicableUsers>)

SETR RACL(MQPROC) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

The following is a sample of the commands required to allow a group (GRP1) to inquire on processes beginning with the letter V on queue manager (QM1):

```
RDEFINE MQPROC QM1.V* UACC(NONE) AUDIT(ALL(READ))
PERMIT QM1.V* CLASS(MQPROC) ID(GRP1) ACCESS(READ)
```

CCI: CCI-000213

Group ID (Vulid): V-6967

Group Title: ZWMQ0056

Rule ID: SV-7548r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0056](#)

Rule Title: WebSphere MQ Namelist resource profiles defined in the MQNLIST Class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- SENSITIVE.RPT(MQNLIST)
- ACF2CMDS.RPT(RESOURCE) Alternate report

b) For all namelist resources (i.e., ssid.namelist) defined to TYPE(MQN) (i.e., MQNLIST resource class), ensure access authorization restricts access to users requiring the ability to make namelist inquiries. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- c) If (b) is true, there is NO FINDING.
- d) If (b) is untrue, this is a FINDING.

Fix Text: A namelist is a MQSeries / WebSphere MQ object that contains a list of queue names. Namelist security validates userids authorized to inquire on namelists. Namelist security will be active, and all profiles ssid.namelist will be defined to the MQNLIST or GMQNLIST class with UACC(NONE) specified. Restrict read access to those userids requiring access to make namelist inquiries.

For all namelist resources (i.e., ssid.namelist) defined to the MQNLIST or GMQNLIST resource classes, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to make namelist inquiries. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
RDEF MQNLIST ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCONN DENY-BY-DEFAULT PROFILE')

RDEF MQNLIST <ssid> ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0056')
PE <ssid> ** CL(MQNLIST) ID(<applicable>)

SETR RACL(MQNLIST) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-6969

Group Title: ZWMQ0057

Rule ID: SV-7550r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0057](#)

Rule Title: WebSphere MQ Alternate User resources defined to MQADMIN resource class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- SENSITIVE.RPT(MQADMIN)
- ACF2CMDS.RPT(RESOURCE) Alternate report

b) For all alternate user resources (i.e., ssid.ALTERNATE.USER.alternatelogonid) defined to TYPE(MQA) (i.e., MQADMIN resource class), ensure access authorization restricts access to users requiring the ability to use the alternate userid. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

c) If (b) is true, there is NO FINDING.

d) If (b) is untrue, this is a FINDING.

Fix Text: Alternate userid security allows access to be requested under another userid. Alternate userid security will be active, and all profiles ssid.ALTERNATE.USER.alternateuserid will be defined to the MQADMIN class with UACC(NONE) specified. Restrict update access to those userids requiring access to alternate userids.

For all alternate user resources (i.e., ssid.ALTERNATE.USER.alternateuserid) defined to the MQADMIN resource class, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to use the alternate userid. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
```

```
RDEF MQADMIN ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN DENY-BY-DEFAULT PROFILE')
```

```
RDEF MQADMIN <ssid>.ALTERNATE.USER.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN DENY-BY-DEFAULT for ALT USER PROFILE')
```

The following is a sample of the commands required to allow payroll server (PAYSRV1) to specify alternate userids starting with the characters PS on queue manager (QM1):

```
RDEFINE MQADMIN QMD1.ALTERNATE.USER.PS* UACC(NONE) AUDIT(ALL)
```

```
PERMIT QMD1.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSRV1) ACCESS(UPDATE)
```

```
SETR RACL(MQADMIN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-6971

Group Title: ZWMQ0058

Rule ID: SV-7552r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0058](#)

Rule Title: WebSphere MQ context resources defined to the MQADMIN resource class are not protected in accordance with security requirements.

Vulnerability Discussion: Context security validates whether a userid has authority to pass or set identity and/or origin data for a message. Context security will be active to avoid security exposure.

This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- SENSITIVE.RPT(MQADMIN)
- ACF2CMDS.RPT(RESOURCE) Alternate report

b) For all context resources (i.e., ssid.CONTEXT) defined to TYPE(MQA) (i.e., MQADMIN resource class, ensure access authorization restricts access to users requiring the ability to pass or set identity and/or origin data for a message. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

c) If (b) is true, there is NO FINDING.

d) If (b) is untrue, this is a FINDING.

Fix Text: Context security validates whether a userid has authority to pass or set identity and/or origin data for a message. Context security will be active, and all profiles ssid.CONTEXT will be defined to the MQADMIN class with UACC(NONE) specified, where ssid is the queue manager name.

Read access is required when the PASS option is specified for an MQOPEN or MQPUT1. Update or control access is required when the SET or OUTPUT option is specified.

For all context resources (i.e., ssid.CONTEXT) defined to the MQADMIN resource class, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to pass or set identity and/or origin data for a message. This is difficult to determine.

However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
```

```
RDEF MQADMIN ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN DENY-BY-DEFAULT PROFILE')
```

```
RDEF MQADMIN <ssid>.CONTEXT UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN PROFILE REQUIRED FOR CONTEXT SECURITY')
```

The following is a sample of the commands required to allow a systems programming group (SYS1) to offload and reload messages for queue manager (QMD1):

```
PERMIT QMD1.CONTEXT CLASS(MQADMIN) ID(SYS1) ACCESS(CONTROL)
```

The following refresh is required for RACListed classes:

```
SETR RACL(MQADMIN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-6973

Group Title: ZWMQ0059

Rule ID: SV-7554r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0059](#)

Rule Title: WebSphere MQ command resources defined to MQCMD resource class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of commands. Failure to properly protect WebSphere MQ Command resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(MQCMDS)
- ACF2CMDS.RPT(RESOURCE) Alternate report

b) For all command resources (i.e., ssid.command) defined to TYPE(MQC) (i.e., MQCMDS resource class, ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Access authorization restricts access to the appropriate personnel as designated in the Websphere MQ COMMAND SECURITY CONTROLS Table in the z/OS STIG Addendum.
 - 2) All command access is logged as designated in the Websphere MQ COMMAND SECURITY CONTROLS Table in the z/OS STIG Addendum.
- c) If both of the items in (b) are true, there is NO FINDING.
- d) If either item in (b) is untrue, this is a FINDING.

Fix Text: Command security validates userids authorized to issue MQSeries / WebSphere MQ commands. Command security will be active

For all command resources (i.e., ssid.command) defined to the MQCMDS resource class, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to the appropriate personnel as designated in the table entitled "Websphere MQ Command Security Controls " in the zOS STIG Addendum.
- 3) All command access is logged as designated in the table entitled "Websphere MQ Command Security Controls" in the zOS STIG Addendum.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
```

```
RDEF MQCMDS ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCMDS DENY-BY-DEFAULT PROFILE')
```

```
RDEF MQCMDSN <ssid>.<CmdName>.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCMDS Required See ZWMQ0059')
```

```
PE <ssid>.<CmdName>.* CL(MQCMDS) ID(<authorizeduser>) ACC(C)
```

```
SETR RACL(MQCMDS) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6975

Group Title: ZWMQ0060

Rule ID: SV-7556r2_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWMQ0060](#)

Rule Title: WebSphere MQ RESLEVEL resources in the MQADMIN resource class are not protected in accordance with security requirements.

Vulnerability Discussion: RESLEVEL security profiles control the number of userids checked for API-resource security. RESLEVEL is a powerful option that can cause the bypassing of all security checks. RESLEVEL security will not be implemented.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(MQADMIN)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZWMQ0060)

b) Ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) A RESLEVEL resource (i.e., ssid.RESLEVEL) is defined for each queue manager to TYPE(MQA) (i.e., MQADMIN resource class) with a default access of PREVENT.
- 2) Access authorization to these RESLEVEL resources restricts all access. No users are permitted access to ssid.RESLEVEL resources.
- c) If both of the items in (b) are true, there is NO FINDING.
- d) If either item in (b) is untrue, this is a FINDING.

Fix Text: RESLEVEL security profiles control the number of userids checked for API-resource security. RESLEVEL security will not be implemented due to the following exposures and limitations:

- (1) RESLEVEL is a powerful option that can cause the bypassing of all security checks.
- (2) Security audit records are not created when the RESLEVEL profile is utilized.
- (3) If the WARNING option is specified on a RESLEVEL profile, no warning messages are produced.

To protect against any profile in the MQADMIN class, such as ssid.**, resolving to a RESLEVEL profile, a ssid.RESLEVEL profile will be defined for each queue manager with UACC(NONE) specified and no users or groups specified in the access list.

Ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) A RESLEVEL resource (i.e., ssid.RESLEVEL) is defined for each queue manager to the MQADMIN resource class with a UACC(NONE).
- 2) Access authorization to these RESLEVEL resources restricts all access. No users or groups must be specified in the access list.

A set of sample commands are provided below to implement the profile necessary for proper security.

```
RDEF MQADMIN <ssid>.RESLEVEL UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN PROFILE REQUIRED BY ZWMQ0060')
```

```
SETR RACL(MQADMIN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

CCI: CCI-001762

UNCLASSIFIED