

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS TSS STIG

Version: 6

Release: 43

24 Jan 2020

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.

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

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(SMPERPT)

b) Invoke the CA-EXAMINE application from within ISPF/PDF. This is typically done by executing %EXAMINE from ISPF/PDF option 6.

From the CA EXAMINE primary menu, enter 2.3.3 from the command line to display the INSTALLED PRODUCTS SELECTION menu. Enter a hyphen (-) for all optional search criteria fields and a valid SMP/E CSI name. Repeat this step for all applicable SMP/E CSI names.

NOTE 1: CSI names can be obtained from the SMPERPT report or by leaving the CSI name field blank and allowing CA-EXAMINE to compile a list of cataloged CSI data sets from which to choose.

NOTE 2: 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 Vendor recommends 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.

Check Content:

This check applies to 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.

For the products in the above category refer to the Vendor's support lifecycle information for current versions and releases. This information should be added to the Vulnerability Questions within the SRRAUDIT Dialog Management document for supported software products.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0012)

If the software products currently running on the reviewed system are at a version greater than or equal to the products listed in the vendor's Support Lifecycle information, this is not 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.

Check Content:

Refer to Vulnerability Questions within the SRRAUDIT Dialog Management document.

Check with the Systems programmer to make sure that a documented migration plan

exists to monitor system software products versions and releases for end-of-life/nonsupport dates. Verify that the procedure notifies management to start procedures to upgrade to supported versions of the products or removal before that date.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0014)

If documented procedures exist to monitor system software products for dates they will become unsupported and to notify management to upgrade to supported versions of the products, this is not a finding.

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

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

Check Content:

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

Check with the Information Assurance Officer to make sure that documented procedures exist for security related software patches to be scheduled, applied and documented.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0018)

b) If documented procedures exist to monitor, apply and document software patches, there is NO FINDING.

c) If documented procedures do not exist to monitor, apply and document software patches, 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.

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

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(PARMLIB) - Refer to the IEASYSxx listing(s).

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0030)
- b) If the LNKAUTH=APFTAB parameter is specified in the IEASYSxx member, there is NO FINDING.
- c) If the LNKAUTH=APFTAB parameter 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.

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

Check Content:

PDI Screen Sort Order: AAMV0040 Default Severity: Category III

a) Refer to the following reports produced by the z/OS Data Collection:

- PARMLIB.ACCESS(IEAAPFxx)
- PARMLIB.ACCESS(PROGxx)

NOTE: The IEAAPFxx and PROGxx reports are only produced if inaccessible libraries exist. The report names represent the actual SYS1.PARMLIB members where inaccessible libraries are found. If these reports do not exist, there is NO FINDING.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0040)

b) If no inaccessible APF libraries exist, there is NO FINDING.

c) If inaccessible APF libraries do exist, this is a FINDING.

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.

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

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(APFDUPS)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0050)

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

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
IFASMFDP IGWSPZAP IHLGTF IMASPZAP IND\$FILE
IOPIOCP IXPIOCP IYPIOCP IZPIOCP WHOIS
LO52INIT 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 is 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-86r4_rule
Severity: CAT II

Rule Version (STIG-ID): AAMV0060
Rule Title: The review of AC=1 modules in APF authorized libraries must be reviewed annually and documentation verifying the modules integrity must be available.

Vulnerability Discussion: The review of AC=1 modules that reside in APF authorized libraries must 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

Check Content:

Refer to the following reports produced by the z/OS Data Collection:

- EXAM.RPT(APFXRPT)

Automated Analysis requires Additional Analysis.

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

- PDI(AAMV0060)

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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(PPTXRPT)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0160)

b) Review the program entries in the CA-EXAMINE PPT LIBRARY SEARCH report.

For all programs not found on the operating system (i.e., missing link date, size, volume, and library name), review their corresponding entries in the CA-EXAMINE PROGRAM PROPERTIES TABLE ANALYSIS report. If a program entry is found with any of the following excessive privileges, ensure that a matching SCHEDxx entry exists for that program revoking these privileges:

- 1) Data set integrity bypass
- 2) Keys 0-7
- 3) Security bypass

c) If a SCHEDxx entry exists for all applicable PPT programs revoking the excessive privileges above, there is NO FINDING.

d) If a SCHEDxx entry does not exist for an applicable PPT program, or does not revoke all the excessive privileges above, this is a FINDING.

Note: Modules for products not in use on the system will have their special privileges explicitly revoked.

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.

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

Check Content:

STIG ID: AAMV0325 Default Severity: Category III Refer to the following reports produced by the z/OS Data Collection:

- PARMLIB.ACCESS(LPALSTxx)
- PARMLIB.ACCESS(IEAFIXxx)
- PARMLIB.ACCESS(IEALPAxx)

NOTE: The LPALSTxx, IEAFIXxx, and IEALPAxx reports are only produced if inaccessible libraries exist. The report names represent the actual SYS1.PARMLIB members where inaccessible libraries are found. If these reports do not exist, there is NO FINDING.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0325)
- b) If no inaccessible LPA libraries exist, there is NO FINDING.
- c) If inaccessible LPA libraries do exist, this is a FINDING.

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:

- LPA1STxx specifies the names of libraries to be concatenated to SYS1.LPA1IB 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 LPA1STxx concatenation, and the LNK1STxx 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 LPA1STxx concatenation
? The LNK1STxx 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 LPA1STxx, 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.

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

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- PARMLIB.ACCESS(LNKLSTxx)

NOTE: The LNKLSTxx reports are only produced if inaccessible libraries exist. The report names represent the actual SYS1.PARMLIB members where inaccessible libraries are found. If these reports do not exist, there is NO FINDING.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0350)

b) If no inaccessible LINKLIST libraries exist, there is NO FINDING.

c) If any inaccessible LINKLIST library exists, this is a FINDING.

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(LNKLSTxx) 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
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3

Check Content:
Refer to the following reports produced by the z/OS Data Collection:

- EXAM.RPT(SMFOPTS)
- EXAM.RPT(PARMLIB) - Alternate report; refer to the SMFPRMxx

listing.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0370)

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.

- 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.

Ensure SMF collection options are specified as stated below with exception of those specified in the above NOTES. 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. (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 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-102r5_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.

Check Content:

Refer to the following reports produced by the z/OS Data Collection:

- EXAM.RPT(SMFOPTS)
- EXAM.RPT(PARMLIB) - Alternate report; refer to the SMFPRMxx listing.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0380)

If all of the required SMF record types identified below are collected, this is not 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
82 (52) – ICSF Statistics
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: 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
82 (52) – ICSF Statistics
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.

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

Check Content:

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

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0400)

b) 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, there is NO FINDING.

c) If it cannot be determined this process exists and is being adhered to, 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 (Vulid): 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.

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

Check Content:

a) 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.

c) If the ACP database is collocated with either it's alternate or backup, this is a 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.

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 can be determined that the ACP database is being backed up on a regularly scheduled basis, there is NO FINDING.

c) If it cannot be determined that the ACP database is being backed up on a regularly scheduled basis, this is a FINDING.

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.

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

Check Content:

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

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0430)

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

c) 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. Backup 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.

IACControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

- a) Refer to the following report produced by the z/OS Data Collection:
- EXAM.RPT(PASSWORD)

Automated Analysis

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

- PDI(AAMV0440)

b) If, based on the information provided, it can be determined that the system PASSWORD data set and OS passwords are not used, there is NO FINDING.

c) If it is evident that OS passwords are utilized, 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.

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

Check Content:

Refer to the following reports produced by the z/OS Data Collection:

- EXAM.RPT(APFXRPT)
- EXAM.RPT(APFTSO)
- EXAM.RPT(IOAPPEND)
- EXAM.RPT(MVSRPT)
- EXAM.RPT(PPTXRPT)
- EXAM.RPT(SVCIBM)
- EXAM.RPT(SVCUSER)
- EXAM.RPT(SVCESR)

If the following items are in effect, this is not a finding:

____ The acquisition of any new IA and IA-enabled Commercial-Off-the-Shelf (COTS) products or any major upgrade meets the applicable Common Criteria, NIAP, or FIPS evaluation and validation requirements specified in CNSSP No. 11 and DODD 8500.1 or receives DAA approval.

____ 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 by the site's system programmer to assure that requirements of CNSSP No. 11 and DODD 8500.1 are met and/or approved by site DAA.

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.

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

Check Content:

Check HMC, VM, and z/OS on how to validate and determine a DASD volume(s) is shared.

Note: In VM issue the command 'QUEUE DASD SYSTEM' this display will show shared volume(s) and indicates the number of systems sharing the volume.

Validate all machines that require access to these shared volume(s) have the volume(s) mounted.

Obtain a map or list VTOC of the shared volume(s).

Check if shared volume(s) contain any critical or sensitive data sets.

Identify shared and critical or sensitive data sets on the system being audited. These data sets can be APF, LINKLIST, LPA, Catalogs, etc, as well as product

data sets.

If all of the critical or sensitive data sets identified on shared volume(s) are protected and justified to be on shared volume(s), this is not a finding.

List critical or sensitive data sets are possible security breaches, if not justified and not protected on systems having access to the data set(s) and on shared volume(s).

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-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.

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(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.

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(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.

IACControls: 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.

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. a

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.

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

Group ID (Vulid): 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.

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:

- SENSITVE.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-71223

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.

Check Content:

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

- SENSITVE.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.

If any of the above is not true, 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-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.

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. C

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.

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(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.

IACControls: 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.

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. s

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.

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-119r4_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.

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITVE.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.

Configure the ESM rules for system catalog to only allow access above "READ" to systems programmers and those authorized by the ISSM/ISSO.

Configure ESM rules for the master catalog to allow access above "READ" to systems programmers ONLY.

Configure ESM rules for the master catalog 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.

All greater than read access must be logged.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-4850

Group Title: ACP00135

Rule ID: SV-4850r3_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.

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.

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.

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.

IACControls: 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:

- SENSITVE.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.

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.

IACControls: 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.

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 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.

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:

- SENSITVE.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.

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.

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:

- SENSITVE.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.

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

Check Content:

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

- SENSITVE.RPT(MVSRPT)

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.

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,
// DPTTY=(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-31712r5_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.

Check Content:

From a command input screen enter:

TSS WHOH IBMFAC(IEAABD.)

Alternately, this can be viewed by following steps:

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

- SENSITVE.RPT(ACP00260)

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 the DEFPROT attribute is specified for the IBMFAC resource class in the RDT and/or that IEAABD. resource and/or generic equivalent is owned. Access will not be given to any user.

___ Ensure that the IEAABD.DMPAUTH. resource and/or generic equivalent access of READ is limited to authorized users.

___ Ensure that the IEAABD.DMPAUTH. resource and/or generic equivalent UPDATE or greater access is restricted to only systems personnel and that all access is logged.

___ Ensure that IEAABD.DMPAKEY. resource and/or generic equivalent specifies that 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 IBMFAC resource class. Ensure that the following are properly specified in the ACP.

(Note: The resources and/or resource prefixes identified below are examples of a possible installation. The actual 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.

If DEFPROT is specified in the IBMFAC RDT the following command examples are not required. To prevent access to these resources, the program dump resources and/or generic equivalent are protected using the following command.

Example:

```
TSS ADDTO(deptacid) IBMFAC(IEAABD.)
```

Ensure that no access is given to IEAABD. resource.

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:

```
TSS PERMIT(authusers) IBMFAC(IEAABD.DMPAUTH.) ACCESS(READ)  
TSS PERMIT(syspauddt) IBMFAC(IEAABD.DMPAUTH.) ACCESS(UPDATE) ACTION(AUDIT)
```

IEAABD.DMPAKEY. access will be restricted to system programming personnel and access will be logged.

Example:

```
TSS PERMIT(syspauddt) IBMFAC(IEAABD.DMPAKEY.) ACCESS(READ) ACTION(AUDIT)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-36
Group Title: ACP00270
Rule ID: SV-6410r7_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.

Check Content:

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

- SENSITVE.RPT(ACP00270)

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 TSS IBMFAC resource class in the RDT has the DEFPROT attribute specified and/or the CSV resources and/or generic equivalent are owned.

___ The TSS resources and/or generic equivalent identified below will be defined with ACTION(AUDIT) and 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.LNKLST

CSVLLA.

___ The TSS CSVDYNEX.LIST resource and/or generic equivalent will be defined with ACTION(AUDIT) and UPDATE access restricted to system programming personnel.

___ The TSS CSVDYNEX.LIST resource and/or generic equivalent will be defined with READ access restricted to auditors.

___ If the products CICS and/or CONTROL-O are on the system, the TSS access to the CSVLLA resource access to the CSVLLA resource and/or generic equivalent will be defined with ACTION(AUDIT) and UPDATE access restricted to the CICS and CONTROL-O STC ACIDs.

If any software product requires access to dynamic LPA updates on the system, the TSS access to the CSVDYLPA resource and/or generic equivalent will be defined with ACTION(AUDIT) 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, UPDATE access can be substituted with ALL or CONTROL. Review the permissions in the TSS documentation when specifying UPDATE.

Fix Text: Ensure that the Dynamic List resources are defined to the IBMFAC 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.
CSVDYLPA.ADD.
CSVDYLPA.ADD.
CSVDYNEX.
CSVDYNEX.LIST
CSVDYNL.
CSVDYNL.UPDATE.LNKLST
CSVLLA.

If DEFPROT is specified in the IBMFAC RDT the following command examples are not required. To prevent access to these resources, the CSV resources are protected using the following commands.

The following commands are provided for example only:

TSS ADDTO(deptacid) IBMFAC(CSV)
or
TSS ADDTO(deptacid) IBMFAC(CSVAPF)
TSS ADDTO(deptacid) IBMFAC(CSVDYLPA)
TSS ADDTO(deptacid) IBMFAC(CSVDYNEX)
TSS ADDTO(deptacid) IBMFAC(CSVDYNL)
TSS ADDTO(deptacid) IBMFAC(CSVDYLPA)
TSS ADDTO(deptacid) IBMFAC(CSVLLA)

Limit authority to those resources to z/OS systems programmers. Restrict to the absolute minimum number of personnel with ACTION(AUDIT) and UPDATE access.

Sample commands are shown here to accomplish this:

TSS PERMIT(syspautd) IBMFAC(CSVAPF.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(syspautd) IBMFAC(CSVAPF.MVS.SETPROG) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(syspautd) IBMFAC(CSVAPF.MVS.SETPROG.FORMAT) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(syspautd) IBMFAC(CSVAPF.MVS.SETPROG.SETPROG.FORMAT.DYNAMIC)
ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(syspautd) IBMFAC(CSVAPF.MVS.SETPROG.SETPROG.FORMAT.STATIC)
ACCESS(UPDATE) ACTION(AUDIT)

The CSVDYLPA.ADD resource will be permitted to BMC Mainview, CA 1, and CA Common Services STC ACIDs with ACTION(AUDIT) and UPDATE access.

The CSVDYLPA resource will be permitted to BMC Mainview, CA 1, and CA Common Services STC ACIDs with ACTION(AUDIT) and UPDATE access.

Sample commands are shown here to accomplish one set of resources:

TSS PERMIT(syspautd) IBMFAC(CSVDYLPA.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(BMC Mainview STC ACID) IBMFAC(CSVDYLPA.ADD.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(CA 1 STC ACID) IBMFAC(CSVDYLPA.ADD.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CCS STC ACID) IBMFAC(CSVDYLPA.ADD.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CA 1 STC ACID) IBMFAC(CSVDYLPA.DELETE.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CCS STC ACID) IBMFAC(CSVDYLPA.DELETE.) ACCESS(UPDATE) ACTION(AUDIT)

The CSVDYNEX.LIST resource and/or generic equivalent will be defined with ACTION(AUDIT) and UPDATE access restricted to system programming personnel.

The CSVDYNEX.LIST resource and/or generic equivalent will be defined with READ access restricted to auditors.

Sample commands are shown here to accomplish this:

TSS PERMIT(syspautd) IBMFAC(CSVDYNEX.) ACCESS(UPDATE) ACTION(AUDIT)

TSS PERMIT(syspau) IBMFAC(CSVL) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(audtaud) IBMFAC(CSVL) ACCESS(READ)

The CSVLLA resource will be permitted to CICS and CONTROL-O STC ACIDs with ACTION(AUDIT) and UPDATE access.

Sample commands are shown here to accomplish one set of resources:

TSS PERMIT(syspau) IBMFAC(CSVLLA.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CICS STC ACIDs) IBMFAC(CSVLLA.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CONTROL-O STC ACID) IBMFAC(CSVLLA.) ACCESS(UPDATE) ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-7482
Group Title: ACP00282
Rule ID: SV-7920r4_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.

Check Content:
From a command screen enter:
TSS WHOHAS OPERCMDS(MVS)

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

- SENSITVE.RPT(ACP00282)
- SENSITVE.RPT(WHOHOPER) – Alternate report

Automated Analysis

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

- PDI(ACP00282)

Access to MVS resource of the OPERCMDS class is restricted to a limited number of authorized users, and all access is logged.

Access to "MVS.**" is not allowed.

Access to z/OS system commands as 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 is true, there is NO FINDING.

Fix Text: Ensure access to the MVS resource of the OPERCMDS class is restricted to a limited number of authorized users, and all access is logged. Ensure access to z/OS system commands as 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).

Ensure no access is granted at level MVS.**.

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.

Example:

TSS ADDTO(deptacid) OPERCMDS(MVS.)

TSS PERMIT(usracid) OPERCMDS(MVS.ACTIVATE) ACTION(AUDIT)

TSS PERMIT(usracid) OPERCMDS(MVS.CANCEL.JOB.) ACTION(AUDIT)

TSS PERMIT(usracid) OPERCMDS(MVS.CONTROL.) ACCESS(UPDATE)
ACTION(AUDIT)

TSS PERMIT(usracid) OPERCMDS(MVS.DISPLAY.) ACCESS(READ)

TSS PERMIT(usracid) OPERCMDS(MVS.MONITOR) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.STOPMN) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-7485
Group Title: ACP00291
Rule ID: SV-7923r4_rule
Severity: CAT II
Rule Version (STIG-ID): ACP00291
Rule Title: CONSOLxx members must be 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.

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: 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 ISSO, "LOGON(AUTO)" may be used. If "LOGON(AUTO)" is used assure that the console userids are defined with minimal access. See ACP00292.

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.

Note: The site should be able to determine the system consoles. However, it is imperative that the site adhere to the "DEFAULT" statement requirement.

CCI: CCI-000382

CCI: CCI-002234

Group ID (Vulid): V-7486
Group Title: ACP00292
Rule ID: SV-7926r3_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.

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 TSS Data Collection and Data Set

and Resource Data Collection:

- TSSCMD5.RPT(@ACIDS)
- SENSITIVE.RPT(WHOHOPER)
- TSSPRIV.RPT

Verify that the MCS console ACIDs 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 TSS ACID.

_____ Each console ACID has no special privileges and/or attributes (e.g., BYPASSING, CONSOLE, etc.).

_____ Each console ACID has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.). Each console can have the Facility of CONSOLE.

_____ Each console ACID will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMD5 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 ACIDs and/or console profile may be given with access READ to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMD5 resource.

Fix Text: The IAO will ensure that all consoles identified in the currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) are defined to the ACP.

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 currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) is associated with a valid TSS ACID.

Each console ACID has no special privileges and/or attributes (e.g., BYPASSING, CONSOLE, etc.).

Each console ACID has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.). Each console can have the Facility of CONSOLE.

Each console ACID will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMD5 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 ACIDs

and/or console profile may be given with access READ to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resource.

Example: (These are only examples, not requirements)

```
TSS CREATE(consnoautolog) TYPE(PROFILE)
NAME('MCS consoles with no autolog')
DEPT('SYS1')
```

```
TSS CREATE(consautolog) TYPE(PROFILE) -
NAME('MCS consoles with autolog') -
DEPT('SYS1')
```

```
TSS CREATE(consname) NAME('MCS console name') -
FACILITY(CONSOLE) PASSWORD(password,0) -
PROFILE(consgroup)
```

```
TSS PER(consautolog) OPERCMDS(MVS.CONTROL) ACCESS(READ)
TSS PER(consautolog) OPERCMDS(MVS.DISPLAY) ACCESS(READ)
TSS PER(consautolog) OPERCMDS(MVS.MONITOR) ACCESS(READ)
TSS PER(consautolog) OPERCMDS(MVS.STOPMN) ACCESS(READ)
```

```
TSS PER(consname) SYSCONS(consname) ACCESS(READ)
```

CCI: CCI-000382

CCI: CCI-002232

Group ID (Vulid): V-7487
Group Title: ACP00293
Rule ID: SV-7929r3_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.

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CONSOLE)

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

- SENSITIVE.RPT(WHOHSYSC)

Automated Analysis

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

- PDI(ACP00293)

Ensure the following items are in effect for all MCS consoles identified in the EXAM.RPT(CONSOLE):

- 1) Each console is defined to SYSCONS resource class and/or the SYSCONS resource class has the DEFPROT attribute.
- 2) The ACID associated with each console has READ access to the corresponding resource defined in the SYSCONS resource class.
- 3) Access authorization for SYSCONS resources restricts access to operations, the Master SCA, and system programming personnel.

Fix Text: The IAO must ensure that all MCS consoles are defined to the SYSCONS 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 TSS SYSCONS resource class and/or the SYSCONS resource class has the DEFPROT attribute.

The ACID associated with each console has access to the corresponding resource defined in the SYSCONS resource class.

Example:

TSS PERMIT(MMGMST) SYSCONS(MMGMST) ACCESS(READ)

Access authorization for SYSCONS resources restricts access to operations, the Master SCA, and system programming personnel.

TSS PERMIT(operaudt) SYSCONS(MMGMST) ACCESS(READ)
TSS PERMIT(Master SCA) SYSCONS(MMGMST) ACCESS(READ)
TSS PERMIT(syspauddt) SYSCONS(MMGMST) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-7488

Group Title: ACP00294

Rule ID: SV-7932r2_rule

Severity: CAT II

Rule Version (STIG-ID): ACP00294

Rule Title: Attributes for Users with the TSO CONSOLE privilege are inappropriate.

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.

Check Content:

a) Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- TSSCMDS.RPT(@PROFS)
- TSSCMDS.RPT(@ACIDS)
- SENSITVE.RPT(WHOHOPER)
- SENSITVE.RPT(WHOHTSOA)

b) If the CONSOLE privilege is not defined to the TSOAUTH resource class, there is NO FINDING (with this specific check).

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 TSO CONSOLE privilege:

- 1) User ACIDs are restricted to the INFO level in the MCSAUTH attribute.
- 2) User ACIDs are restricted to READ access to the MVS.MCSOPER.acid resource defined in the OPERCMDS resource class.
- 3) User ACIDs and/or profile ACIDs are restricted to the CONSOLE resource defined in the TSOAUTH resource class.

d) If all of the above in (c) are true, there is NO FINDING.

e) If any of the above in (c) 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.

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 TSO CONSOLE privilege: a) User ACIDs are restricted to the INFO level in the MCSAUTH attribute. b) User ACIDs are restricted to READ access to the MVS.MCSOPER.acid resource defined in the OPERCMDS resource class. c) User ACIDs and/or profile ACIDs are restricted to the CONSOLE resource defined in the TSOAUTH resource class.

For Example:

```
TSS ADDTO (userid) MCSAUTH(INFO)
TSS PERMIT(userid) OPERCMDS(MVS.MCSOPER.userid)
    ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(oprprofileacid) TSOAUTH(CONSOLE)
    ACCESS(READ) ACTION(AUDIT)
```

CCI: CCI-000213

Group ID (Vulid): V-7558

Group Title: ACP00310

Rule ID: SV-8037r2_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.

Check Content:

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

- TSSCMDS.RPT(UNUSED35)

b) If every user shows a LAST-USED=yy.ddd within the past 35 days, there is NO FINDING.

c) If the above is untrue, this is a FINDING.

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.

Check Content:

Examine the documented process for audit trail reviews as well as the audit trail showing the reviews to ensure reviews and analysis of information system audit records are performed every seven days or more frequently if required by the site Security 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/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' 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

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, this is not a 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.

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

- a) 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 will 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.

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

Check Content:

Note: For DISA sites the product used to generate these reports is CA-Auditor.

z/OS Baseline Reporting – Review period is based upon 10% random selection of z/OS Domains at the given site by the IAO. Such schedule shall not be published or known – selection of z/OS domains shall be randomly selected each week.

a) The z/OS Baseline reports (as identified by report/function CS212C (Updates to SYS1.PARMLIB), CS221C (APF library statistics) and CS243C (LPA library statistics) shall be reviewed and validated with the appropriate system programming staff on a weekly schedule, or as required based on INFOCON Level requirements.

Note: Sites that do not utilize CA-Auditor, review the z/OS STIG Addendum for the samples of the CA-Auditor report to identify the information to collect. The INFOCON Level requirements can be found in STRATEGIC COMMAND DIRECTIVE (SD) 527-1.

b) Such 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.

c) If the baseline reports are being reviewed and samples of the baseline reports exist, there is NO FINDING.

d) 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-38888r5_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 symbolic. This exposure may threaten the integrity and availability of the operating system environment.

Check Content:

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

- SENSITVE.RPT(WHOHIBMF)

Automated Analysis

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

- PDI(ACP00350)

Verify that the accesses for IEASYMUP resources and/or generic equivalent are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS resources are owned or DEFPROT is specified for the resource class.

___ The TSS resource access authorizations restrict UPDATE and/or greater access to DASD administrators, Tape Library personnel, and system programming personnel.

___ The TSS resource logging requirements are specified.

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:

```
TSS ADD(ADMIN) IBMFAC(IEASYMUP)
```

```
TSS PERMIT(<dasdaudt>) IBMFAC(IEASYMUP) ACC(U) ACTION(AUDIT)
```

```
TSS PERMIT(<syspauadt>) IBMFAC(IEASYMUP) ACC(U) ACTION(AUDIT)
```

```
TSS PERMIT(<tapeaudt>) IBMFAC(IEASYMUP) ACC(U) ACTION(AUDIT)
```

CCI: CCI-002234

Group ID (Vulid): V-69223

Group Title: ICER0010

Rule ID: SV-83833r1_rule

Severity: CAT II

Rule Version (STIG-ID): ICERT010

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.

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:

TSSCMDS.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: ICER0020

Rule ID: SV-83843r1_rule

Severity: CAT II

Rule Version (STIG-ID): ICERT020

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.

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:

TSSCMDS.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.

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: ICER0030

Rule ID: SV-83849r1_rule

Severity: CAT II

Rule Version (STIG-ID): ICERT030

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.

Check Content:

If certificate name filtering is in use, the ISSM should document each active filter rule and have written approval to use the rule.

Issue the following TSS command to list any certificate name filters defined to TSS:

```
TSS LIST(SDT) CERTMAP(ALL)
```

If there is nothing to list, there is not a finding.

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

If certificate name filters are defined and they have a Status of TRUST, certificate name filtering is in use.

If certificate name filtering is in use and filtering rules have been documented and approved by the ISSM, there is not a finding.

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 (Vulid): V-3233

Group Title: IFTP0010

Rule ID: SV-13260r2_rule

Severity: CAT II

Rule Version (STIG-ID): IFTP0010

Rule Title: The FTP Server daemon is defined improperly.

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.

Check Content:

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

- TSSCMD5.RPT(@ACIDS)

- TSSCMDS.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 ACID is FTPD.

3) The FTPD ACID has the STC facility.

4) The FTPD ACID 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: a (Manual) - Review the FTP Server daemon account, privileges, and access authorizations defined to the ACP. 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 ACID is FTPD.

3) The FTPD ACID has the STC facility.

4) The FTPD ACID has the following z/OS UNIX attributes:
UID(0), HOME directory '/', shell program /bin/sh.

For example:

```
TSS CREATE(FTPD) TYPE(USER) NAME(FTPD)
DEPT(existing-dept) FACILITY(STC) PASSWORD(password,0)
TSS ADD(FTPD) DFLTGRP(STCTCPX) GROUP(STCTCPX)
TSS ADD(FTPD) SOURCE(INTRDR)
TSS ADD(FTPD) UID(0) HOME(/) OMVSPGM(/bin/sh)
TSS ADD(FTPD) MASTFAC(TCP)
TSS ADD(STC) PROCNAME(FTPD) ACID(FTPD)
TSS PERMIT(FTPD) IBMFAC(BPX.DAEMON) ACCESS(READ)
```

TSS PERMIT(FTPD) IBMFAC(BPX.POE) ACCESS(READ)
TSS PERMIT(FTPD) SERVAUTH(EZB.STACKACCESS.)ACCESS(READ)

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.

IACControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

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.

Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFTP0020)

b) Ensure the following items are in effect for 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.
- 2) The ANONYMOUS keyword is not coded on the PARM parameter on the EXEC statement.
- 3) The ANONYMOUS=logonid combination is not coded on the PARM parameter on the EXEC statement.
- 4) The INACTIVE keyword is not coded on the PARM parameter on the EXEC statement.

c) 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.

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 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: 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.

CCI: CCI-000366

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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFTP0030)

b) 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.

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).

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.

4) The BANNER statement is coded.

c) If all of the above are true, there is NO FINDING.

d) If any of the above is untrue, this is a FINDING.

FTP.DATA CONFIGURATION STATEMENTS

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

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-3236r3_rule

Severity: CAT II

Rule Version (STIG-ID): IFTP0040

Rule Title: User exits for the FTP Server must not be used without proper approval and 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.

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: 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 none 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-3237r3_rule

Severity: CAT II

Rule Version (STIG-ID): IFTP0050

Rule Title: The warning banner for the FTP Server must be 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

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(IFTPO050)

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: 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.

IAControls: DCCS-1, DCCS-2, ECAT-1, ECAT-2

Check Content:

Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFT0060)

Ensure the following configuration statement settings are in effect in the FTP Data configuration data set. If the following guidance is true, this is not a finding.

Ensure the following items are in effect for the configuration statements specified in the FTP Data configuration file:

- ___ The SMF statement is coded with a value of TYPE119.
- ___ The SMFJES and SMFSQL statements are coded without any additional values.
- ___ The SMFAPPE, SMFDEL, SMFEXIT, SMFLOGN, SMFREN, SMFRETR, and SMFSTOR statements are not coded or commented out.

FTP.DATA Configuration Statements

```
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]
```

Note: SMF, SMFJES, and SMFSQL may be duplicated in configuration, but one of the entries must specify TYPE119.

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.

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

Check Content:

Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(IFT0070)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(IFT0070)

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.

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
```

NOTES: Some of the files listed above are not used in every configuration. The absence of a file is not considered a finding.

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 /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 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 permission bits for /usr/sbin/tftpd should be set to 644.

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. Also, the permission bit setting for this file must be set as indicated in the table above. A more restrictive set of permissions is not permitted.

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 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.

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

Check Content:

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

- SENSITIVE.RPT(FTPRPT)

Automated Analysis

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

- PDI(IFTP0080)

b) Ensure the following data set controls are in effect for the FTP

Server:

1) WRITE and ALLOCATE access to the data set containing the FTP Data configuration file is restricted to systems programming personnel.

NOTE: READ access to all authenticated users is permitted.

2) WRITE and ALLOCATE access to the data set containing the FTP Data configuration file is logged.

3) WRITE and ALLOCATE access to the data set containing the FTP banner file is restricted to systems programming personnel.

4) 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.

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

c) 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

Group ID (Vulid): V-3241

Group Title: IFTP0090

Rule ID: SV-6925r2_rule

Severity: CAT II

Rule Version (STIG-ID): IFTP0090

Rule Title: The TFTP Server program is controlled improperly.

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.

Check Content:

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

- TSSCMDS.RPT(WHOOPGM)
- SENSITVE.RPT(WHOHPGM)

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) Program resources TFTPDP and EZATD are owned appropriately in the PROGRAM resource class.
- 2) 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 in (b) is untrue, this is a FINDING.

Fix Text: Evaluate the impact of implementing the following change. Develop a plan of action and implement the change as required. Ensure that the EZATD program and its alias TFTPDP are defined to CA-TSS and no access to the program

resources TFTPd and EZATD is permitted. The following commands provide a sample of how to protect the TFTP server program by assigning ownership and no permissions: TSS ADD(ADMIN) PROGRAM(TFTPd,EZATD)

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.

IACControls: DCCS-1, DCCS-2, EBRU-1, ECCT-1, ECCT-2

Check Content:

- a) Provide a list of all FTP userids defined to the ACP database, including the function and purpose of each FTP userid.
- b) Refer to the above list
- c) Ensure that an Acknowledgement of Risk Letter exist for all userids utilizing unencrypted communications.
- d) If (c) is true, there is NO FINDING.
- e) If (c) 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.

IAControls: IAIA-1, IAIA-2

Check Content:

Provide a list(s) of the locations for all FTP Control cards within a given application/AIS, ensuring no FTP control cards are within in-stream JCL, JCL libraries or any open access datasets. List shall indicate which application uses the PDS, and access requirements for those PDS's (who and what level of access). Lists/spreadsheet used for documenting the meeting of this requirement shall be maintained by the responsible Application/AIS Team, available upon request and not maintained by DISA Mainframe IAO.

Refer to the to the above list

Access to FTP scripts and/or data files located on host system(s) that contain FTP userid and or password will be restricted to those individuals responsible for the application connectivity and who have a legitimate requirement to know the userid and password on a remote system.

FTP Control Cards within In-stream JCL, within JCL libraries or open access libraries/datasets is a finding.

Anyone having access of read or greater to the FTP control cards not listed

within the spreadsheet by userid 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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(ERC)

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(PARMLIB)

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.

b) If the Syslog daemon SYSLOGD is started automatically during the initialization of the z/S/ system, there is NO FINDING.

c) If (b) 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-7080r3_rule

Severity: CAT II

Rule Version (STIG-ID): ISLG0020

Rule Title: The Syslog daemon must be defined properly.

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.

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(OMVSUSER)

Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(ERC) - Refer to this report if the Syslog daemon is started from /etc/rc.

Refer to the JCL procedure libraries defined to JES2.

Ensure that the Syslog daemon is properly defined and protected as stated below. If the following guidance is true, this is not a finding.

- ___ The Syslog daemon userid is SYSLOGD.
- ___ The SYSLOGD userid has the STC facility.
- ___ The SYSLOGD userid has UID(0), HOME('/'), and PROGRAM('/bin/sh') specified in the OMVS segment.
- ___ The SYSLOGD started proc is assigned the SYSLOGD userid is in the Started Task Table.
- ___ If Syslog daemon is started from /etc/rc then ensure that the _BPX_JOBNAME and _BPX_USERID environment variables are assigned a value of SYSLOGD.

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 has the STC facility.
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:

```
TSS CREATE(SYSLOGD) TYPE(USER) NAME(SYSLOGD) –  
DEPT(existing-dept) FACILITY(STC) –  
PASSWORD(password,0)  
TSS ADD(SYSLOGD) DFLTGRP(stctcpx) GROUP(stctcpx)  
TSS ADD(SYSLOGD) SOURCE(INTRDR)  
TSS ADD(SYSLOGD) UID(0) HOME(/) OMVSPGM(/bin/sh)
```

The SYSLOGD started proc is assigned the SYSLOGD userid is in the Started Task Table.

TSS ADD(STC) PROCNAME(SYSLOGD) ACID(SYSLOGD)

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.

IACControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:

Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(ISLG0030)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ISLG0030)

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.

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
```

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

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
chmod rwx=f /usr/lpp/tcpip/sbin/syslogd
chmod 0744 /etc/syslog.conf
chmod w=sf,rx+f /etc/syslog.conf
chmod 0744 /log_dir/log_file
chmod 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.

IAControls: DCCS-1, DCCS-2

Check Content:

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.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITCP0010)

b) 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-3216r4_rule

Severity: CAT II

Rule Version (STIG-ID): ITCP0020

Rule Title: TCPIP.DATA configuration statements for the TCP/IP stack must 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.

Check Content:

Refer to the Data configuration file specified on the SYSTCPD DD statement in the TCPIP started task JCL.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITCP0020)

Verify that the following configuration statements are specified in the TCP/IP Data configuration file. If the following guidance is true, this is not a finding.

TCPIPJOBNAME

HOSTNAME

DOMAINORIGIN/DOMAIN (The DOMAIN statement is functionally equivalent to the DOMAINORIGIN Statement)

DATASETPREFIX

Fix Text: 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-5627r4_rule

Severity: CAT II

Rule Version (STIG-ID): ITCP0025

Rule Title: The hosts identified by the NSINTERADDR statement must 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

Check Content:

Refer to the Data configuration file specified on the SYSTCPD DD statement in the TCPIP started task JCL.

Gather the following information for any NSINTERADDR statement coded in the TCP/IP Data configuration file:

Identify the physical location of the host running a DNS server (i.e., on-site or off-site at organization, city, state).

Obtain the description of the physical security controls used to limit access to the area where the host is located.

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITCP0025)

Verify that if the NSINTERADDR statements are not specified in the TCP/IP Data configuration file, this is not applicable.

Verify that the NSINTERADDR statements specified in the TCP/IP Data configuration file. If the following guidance is true, this is not a finding.

___ The NSINTERADDR statements refer to hosts connected directly to networks within the physical premises of the host site.

___ The NSINTERADDR statements refer to hosts that are located in areas with physical access limited to authorized personnel.

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.

IACControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the Profile configuration file specified on the PROFILE DD

statement in the TCPIP started task JCL.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITCP0030)

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.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance in STIG ID ITCP0070.

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:

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 IBM's 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.

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(ITCP0040)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ZTCP0040)

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.

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

NOTE:

Some of the files listed above are not used in every configuration. Absence of any of the files is not considered 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 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
chmod w=sf,rx+f /etc/hosts
chmod 0744 /etc/protocol
chmod w=sf,rx+f /etc/protocol
chmod 0744 /etc/resolv.conf
chmod w=sf,rx+f /etc/resolv.conf
chmod 0740 /etc/services
chmod w=sf,rx+f /etc/services
chmod 0755 /usr/lpp/tcpip/bin
chmod 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-7084r5_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.

Check Content:

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

- SENSITVE.RPT(ITCP0050)

Automated Analysis requires Additional Analysis.

Automated Analysis

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

- PDI(ITCP0050)

Ensure that all TCP/IP 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 EZA, EZB, and IST resources of the SERVAUTH resource class are properly owned and/or DEFPROT is specified in the SERVAUTH resource class.

___ No access is given to the EZA, EZB, and IST high level 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.

____ If the product CSSMTP is on the system, 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.

____ Authenticated users that require access will be 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.

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 of the SERVAUTH resource class are properly owned and/or DEFPROT is specified in the SERVAUTH resource class.

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:

```
TSS ADD(ADMIN) SERVAUTH(EZB)
```

or

```
TSS REPLACE(RDT) RESCLASS(SERVAUTH) ATTR(DEFPROT)
```

```
TSS PER(authusers) SERVAUTH(EZB.CSSMTP.sysname.writernode) ACCESS(READ)
```

```
TSS PER(authusers) SERVAUTH(EZB.FTP.) ACCESS(READ)
```

```
TSS PER(ftpprofile)SERVAUTH(EZB.FTP.sysname.ftpstc.ACCESS.HFS)ACC(READ)
```

```
TSS PER(authusers) SERVAUTH(EZB.NETACCESS.) ACCESS(READ)
```

```
TSS PER(authusers) SERVAUTH(EZB.PORTACCESS.) ACCESS(READ)
```

```
TSS PER(authusers) SERVAUTH(EZB.STACKACCESS.) ACCESS(READ)
```

```
TSS PER(ftpprofile)SERVAUTH(EZB.STACKACCESS.sysname.TCPIP)ACC(READ)
```

The following notes apply to these controls:

- According to Computer Associates' Security Cookbook for eTrust CA TOP SECRET, access to stack (EZB.STACKACCESS) resources will be given to ACIDs that require it. As a result, adequate access definitions for stack resources are critical to proper system availability. 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-7088r3_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.

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(OMVSUSER)

b) Ensure the following items are in effect for the ACID(s) assigned to the

TCP/IP address space(s):

1) Named TCPIP or, in the case of multiple instances, prefixed with TCPIP.

2) Has the STC facility.

3) z/OS UNIX attributes:

UID(0), HOME directory '/', shell program /bin/sh

c) Ensure the following items are in effect for the ACID assigned to the EZAZSSI started task:

1) Named EZAZSSI

2) Has the STC facility.

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: Develop a plan of action to implement the required changes. Ensure the following items are in effect for the ACID(s) assigned to the TCP/IP address space(s):

1) Named TCPIP or, in the case of multiple instances, prefixed with TCPIP

2) Has the STC facility.

3) z/OS UNIX attributes: UID(0), HOME directory '/', shell program /bin/sh

Ensure the following items are in effect for the ACID assigned to the EZAZSSI started task:

1) Named EZAZSSI

2) Has the STC facility

For Example:

The following commands can be used to create the user accounts and assign the privileges that are required for the TCP/IP address space and the EZAZSSI started task:

```
TSS CREATE(TCPIP) TYPE(USER) NAME(TCPIP)
    DEPT(existing-dept) FACILITY(STC) PASSWORD(password,0)
TSS ADD(TCPIP) DFLTGRP(STCTCPX) GROUP(STCTCPX)
```

```
TSS ADD(TCPIP) SOURCE(INTRDR)
TSS ADD(TCPIP) UID(0) HOME(/) OMVSPGM(/bin/sh)
TSS ADD(TCPIP) MASTFAC(TCP)
TSS ADD(STC) PROCNAME(TCPIP) ACID(TCPIP)
TSS PERMIT(TCPIP) IBMFAC(BPX.DAEMON) ACCESS(READ)

TSS CREATE(EZAZSSI) TYPE(USER) NAME(EZAZSSI)
    DEPT(existing-dept) FACILITY(STC) PASSWORD(password,0)
TSS ADD(EZAZSSI) DFLTGRP(STCTCPX) GROUP(STCTCPX)
TSS ADD(EZAZSSI) SOURCE(INTRDR)
TSS ADD(EZAZSSI) UID(non-zero) HOME(/) OMVSPGM(/bin/sh)
TSS ADD(EZAZSSI) MASTFAC(TCP)
TSS ADD(STC) PROCNAME(EZAZSSI) ACID(EZAZSSI)
```

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 IBM's 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.

IACControls: 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(TCPRPT)

Automated Analysis

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

- PDI(ITCP0070)

b) Ensure the following data set controls are in effect for the Base TCP/IP component:

1) 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).

2) 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.

3) 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.

4) WRITE and ALLOCATE 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.

NOTE: For systems running the TSS ACP replace the WRITE and ALLOCATE with WRITE, UPDATE, CREATE, CONTROL, SCRATCH, and ALL.

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-3222r3_rule

Severity: CAT II

Rule Version (STIG-ID): ITNT0010

Rule Title: PROFILE.TCPIP configuration statements for the TN3270 Telnet Server must be 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.

Check Content:

a) Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITNT0010)

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.

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.

- 2) The TELNETPARMS TKOSPECLURECON statement is not coded or commented out.

BEGINVTAM Block (one or more defined)

- 1) 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.

CCI: CCI-000764

Group ID (Vulid): V-3223

Group Title: ITNT0020

Rule ID: SV-3223r4_rule

Severity: CAT II

Rule Version (STIG-ID): ITNT0020

Rule Title: VTAM session setup controls for the TN3270 Telnet Server must be 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

Check Content:

a) Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

Automated Analysis requires Additional Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITNT0020)

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.
- 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.
- 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.

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.

IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:

a) Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

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.

IACControls: DCCS-1, DCCS-2, ECMT-2, ECTM-1

Check Content:

Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

Automated Analysis

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITNT0050)

If the following items are in effect for the configuration specified in the TCP/IP Profile configuration file, this is not a finding.

NOTE: If an 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.

NOTE: FIPS 140-2 minimum encryption is the accepted level of encryption and will override this requirement if greater.

___ The TELNETGLOBALS block that specifies an ENCRYPTION statement states one or more of the below cipher specifications.

___ Each TELNETPARMS block that specifies the SECUREPORT statement, specifies an ENCRYPTION statement states one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

Cipher Specifications

SSL_3DES_SHA

SSL_AES_256_SHA

SSL_AES_128_SHA

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.

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

Check Content:

Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

Automated Analysis.

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ITNT0060)
- PDIX(ITNT0060) Note: Created when sites have multiple TCP/IP and FTP started task procedures.

Ensure the following configuration statement settings are in effect in the TCP/IP Profile configuration data set. If the following guidance is true, this is not a finding.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration data set, 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.

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.

IACControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(EINETD)

b) If the otelnetd command specifies OMVS or OMVSKERN as the user, there is NO FINDING.

c) If the otelnetd command specifies any user other than OMVS or OMVSKERN, 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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(EINETD)

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-3231r3_rule

Severity: CAT II

Rule Version (STIG-ID): IUTN0030

Rule Title: The warning banner for the z/OS UNIX Telnet Server must be 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

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.

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/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

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/otelnetsd
chaudit rwx=f /usr/lpp/tcpip/sbin/otelnetsd
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-7493
Group Title: TSS0246
Rule ID: SV-7938r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0246
Rule Title: Operating system commands (MVS.) of the OPERCMDS resource class are not properly owned..

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.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(WHOOOPER)

Automated Analysis

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

- PDI(TSS0246)

b) Review ownership of the MVS. resource in the OPERCMD5 class.

c) If the (MVS.) resource is owned by the OPERCMD5 class, and/or the DEFPROT attribute is specified for the OPERCMD5 resource class in the RDT, there is NO FINDING.

d) If the (MVS.) resource is not owned or the OPERCMD5 class does not have DEFPROT as mentioned in (c) above, or is inappropriately owned, this is a FINDING.

Fix Text: z/OS system command controls are provided via resources in the OPERCMD5 resource class. The IAO will ensure that (MVS.) of the OPERCMD5 resource class are properly owned or at a minimum the OPERCMD5 resource in the RDT specifies the DEFPROT attribute. Name the actual owning ACID specified for deptacid in accordance with installation recommendations.

When protecting the facilities for z/OS system commands via the OPERCMD5 class, use the following controls:

(1) Prevent access to the z/OS resources by default, and log all access. Create generic and specific permissions with logging as required using the required controls for z/OS System Commands listed in ACP00282.

For example:

TSS ADDTO(deptacid) OPERCMD5(MVS.)

TSS PERMIT(usracid) OPERCMD5(MVS.ACTIVATE) ACTION(AUDIT)

TSS PERMIT(usracid) OPERCMDS(MVS.CANCEL.JOB.) ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.CONTROL.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.DISPLAY.) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.MONITOR) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.STOPMN) ACCESS(READ)

CCI: CCI-000213

Group ID (Vulid): V-70
Group Title: TSS0249
Rule ID: SV-70r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0249
Rule Title: The ADMINBY Control Option is not set to ADMINBY.

Vulnerability Discussion: The ADMINBY Control Option enables administrative information to be recorded for facilities added and resources permitted.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0249)

b) If the ADMINBY Control Option value is specified, there is NO FINDING.

c) If the ADMINBY Control Option value is not set or set to NOADMBY, this is a FINDING.

Fix Text: The IAO will ensure ADMINBY control option is set to Adminby to record who when and where information in the ACID security record for administrative changes.

Evaluate the impact associated with implementation of the control option.

Develop a plan of action to implement the control option setting ADMINBY and proceed with the change.

CCI: CCI-002234

Group ID (Vulid): V-188

Group Title: TSS0250

Rule ID: SV-188r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0250

Rule Title: The ADSP (Automatic Data Set Protection) Control Option is not set to (NO).

Vulnerability Discussion: The ADSP Control Option allows the TSS administrator to determine whether newly created data sets will be automatically protected.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0250)

b) If the ADSP Control Option value is set to ADSP(NO), there is NO FINDING.

c) If the ADSP Control Option value is NOT set to ADSP(NO), this is a FINDING.

Fix Text: The IAO will ensure ADSP control option is set to (NO) indicating that the RACF bit in the DSCB will not be set. Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to ADSP(NO) and proceed with the change.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-189

Group Title: TSS0260

Rule ID: SV-189r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0260

Rule Title: The AUTH Control Option values specified are not set to (OVERRIDE,ALLOVER) or (MERGE,ALLOVER).

Vulnerability Discussion: The AUTH Control Option indicates whether TSS will merge the user, profile, and all record for its access search, or whether TSS will search each one separately.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0260)

b) If the AUTH Control Option values are set to AUTH(OVERRIDE, ALLOVER) or AUTH(MERGE, ALLOVER), there is NO FINDING.

c) If the AUTH Control Option values are not set to AUTH(OVERRIDE, ALLOVER) or AUTH(MERGE, ALLOVER), this is a FINDING.

Fix Text: The IAO will ensure AUTH control option is set to (OVERRIDE, ALLOVER) or (MERGE, ALLOVER). With (OVERRIDE, ALLOVER), TSS separately searches first the user, then profiles, and then the ALL record for its access authorization. With (MERGE, ALLOVER), TSS merges and searches the user and all profiles, and then the ALL record for its access authorization. Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to AUTH(OVERRIDE, ALLOVER) or AUTH(MERGE, ALLOVER) and proceed with the change.

CCI: CCI-000213

Group ID (Vulid): V-190

Group Title: TSS0270

Rule ID: SV-190r4_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0270

Rule Title: The AUTOERASE Control Option must be set to (ALL) for all systems.

Vulnerability Discussion: AUTOERASE will force TSS to erase all residual information on DASD.

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 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 migration process or contingency plan activation.

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis requires Additional Analysis.

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

- PDI(TSS0270)

If the AUTOERASE Control Option value is set to ALL, this is not a finding.

Fix Text: The IAO must ensure AUTOERASE control option is set to (ALL) for all systems to erase all residual information on DASD. Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the AUTOERASE control option to (ALL) for all systems and implement.

CCI: CCI-001028

CCI: CCI-001090

Group ID (Vulid): V-68

Group Title: TSS0275

Rule ID: SV-68r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0275

Rule Title: The CANCEL Control Option value specified is set to CANCEL.

Vulnerability Discussion: The CANCEL Control Option allows security administrators to use the O/S CANCEL command to bring the TSS address space down.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0275)

If the CANCEL Control Option is not specified, this is not a finding.

Fix Text: Remove the CANCEL sub-option from the Control Options list.

TSS MODIFY(control_option [(suboption_list)])

CCI: CCI-000336

CCI: CCI-000366

CCI: CCI-002357

Group ID (Vulid): V-191

Group Title: TSS0280

Rule ID: SV-191r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0280

Rule Title: The CPFRCVUND Control Option value specified is not set to (NO).

Vulnerability Discussion: The CPFRCVUND Control Option indicates whether or not the local node can receive commands propagated from nodes which have not been defined to the CPFNODES list.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0280)

b) If the CPFRCVUND Control Option value is set to NO, There is NO FINDING.

c) If the CPFRCVUND Control Option value is set to YES, this is a FINDING.

Fix Text: The IAO will ensure CPFRCVUND control option is set to (NO). Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the control option setting to NO and proceed with the change.

CCI: CCI-001762

Group ID (Vulid): V-25483

Group Title: TSS0290

Rule ID: SV-31681r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0290

Rule Title: The CPFTARGET Control Option value specified is not set to (LOCAL).

Vulnerability Discussion: The CPFTARGET Control Option indicates whether or not commands are to be propagated to other nodes which are defined to the CPFNODES list or DEFNODES associated with the ACID.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0290)

Ensure the CPFTARGET Control Option value is set to LOCAL.

Fix Text: The IAO will ensure CPFTARGET control option is set to (LOCAL).
Evaluate the impact associated with implementation of the control option.
Develop a plan of action to set the control option setting to LOCAL and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-193
Group Title: TSS0320
Rule ID: SV-193r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0320
Rule Title: The DEBUG Control Option value is not set to (OFF).

Vulnerability Discussion: The DEBUG Control Option controls the production of debugging dumps used to determine the cause of abnormal error conditions.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis Refer to the following report produced by the TSS Data Collection:

- PDI(TSS0320)

b) If the DEBUG Control Option value is set to OFF, there is NO FINDING.

c) If the DEBUG Control Option value is set to ON, this is a FINDING

Fix Text: The IAO will ensure DEBUG control option is set to (OFF). Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the DEBUG control option setting to (OFF) and proceed with the change.

CCI: CCI-002883

Group ID (Vulid): V-194

Group Title: TSS0330

Rule ID: SV-194r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0330

Rule Title: TSS MODIFY output must specify ACTIVE DIAGTRAP ENTRIES: ON = 00.

Vulnerability Discussion: The DIAGTRAP Control Option is used to produce a diagnostic dump.

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 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 migration process or contingency plan activation.

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis requires Additional Analysis.

Automated Analysis

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

- PDI(TSS0330)

b) If the ACTIVE DIAGTRAP Control Option values listing from TSS MODIFY are: "ACTIVE DIAGTRAP ENTRIES: ON = 00", there is NO FINDING.

c) If the ACTIVE DIAGTRAP Control Option value listing from TSS MODIFY is NOT: "ACTIVE DIAGTRAP ENTRIES: ON = 00", this is a FINDING.

NOTE: An active trap may be set if working on a problem with CA and then "ON ="

will contain a non zero value. There must be an open issue with CA to justify.

Fix Text: Ensure DIAGTRAP control option is either not specified or is set to DIAGTRAP(ALL,DEL) in TSS PARMLIB. Also, issue a TSS MODIFY command and ensure the following is listed:

"ACTIVE DIAGTRAP ENTRIES: ON = 00"

Issue the following to delete all existing diagtraps:

TSS MODIFY(DIAGTRAP(ALL,DEL))

A trap may be set and active if working a current issue with CA and CA requested a DIAGTRAP be set.

CCI: CCI-000366

Group ID (Vulid): V-195

Group Title: TSS0350

Rule ID: SV-195r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0350

Rule Title: The DL1B Control Option is not set to (NO).

Vulnerability Discussion: The DL1B Control Option is used to implement PSB and DBD security for IMS batch regions, and to provide access to the TSS application interface program.

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 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 migration process or contingency plan activation.

IACControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0350)

b) If the DL1B Control Option value is set to DL1B(NO), there is NO FINDING.

c) If the DL1B Control Option value is set to DL1B(YES), this is a FINDING.

Fix Text: The IAO will ensure DL1B control option is set to (NO) Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the control option value to DL1B(NO) and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-196

Group Title: TSS0360

Rule ID: SV-196r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0360

Rule Title: The DOWN Control Option values specified are not set to (BW,SB,OW) and TW if users are still defined in SYS1.UADS, TN if only systems personnel are defined in SYS1.UADS.

Vulnerability Discussion: The DOWN Control Option determines how jobs are initiated and passwords changed when the TSS address space is inactive.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0360)

b) If only systems personnel are defined in SYS1.UADS and the DOWN Control Option values are set to DOWN(BW,SB,TN,OW), there is NO FINDING.

c) If non systems personnel are defined in SYS1.UADS and the DOWN Control Option values are set to DOWN(BW,SB,TW,OW), there is NO FINDING.

d) If the DOWN Control Option values do not conform to the above requirements, this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified below and proceed with the change.

Setting if ONLY systems personnel are defined in SYS1.UADS: DOWN(BW,SB,TN,OW)

Setting if any non systems personnel are defined in SYS1.UADS: DOWN(BW,SB,TW,OW)

CCI: CCI-001190

CCI: CCI-001665

Group ID (Vulid): V-197

Group Title: TSS0380

Rule ID: SV-197r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0380

Rule Title: The EXIT Control Option is not set to (ON) for DISA sites.

Vulnerability Discussion: The EXIT Control Option activates and deactivates the installation exit. For non DISA sites this value is site defined. DISA sites use NCPASS.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

NOTE: For non DISA sites EXIT is site defined. DISA sites use NCPASS TOKENs requiring an installation EXIT.

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0380)

b) If the EXIT Control Option is set to EXIT(ON), there is NO FINDING.

c) If the EXIT Control Option is NOT set to EXIT(ON), this is a FINDING.

Fix Text: For DISA sites and sites requiring an installation exit, set the EXIT control option to: EXIT(ON)

CCI: CCI-000764

CCI: CCI-000765

Group ID (Vulid): V-15098

Group Title: TSS0385

Rule ID: SV-15870r2_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0385

Rule Title: The Facility Control Option does not specify the sub option of MODE=FAIL.

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 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 or sub options introduces the possibility of exposure during migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(FACALL)

Automated Analysis

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

- PDI(TSS0385)

b) If the FACILITY Control Option specifies the sub option of MODE=FAIL there is NO FINDING.

c) If the FACILITY Control Option does not specifies the sub option of MODE=FAIL , this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the FACILITY Control Option MODE sub-option. Develop a plan of action to implement the FACILITY Control Option MODE sub-option setting to MODE=FAIL and proceed with the change.

CCI: CCI-000366

CCI: CCI-002357

CCI: CCI-002358

Group ID (Vulid): V-198

Group Title: TSS0390

Rule ID: SV-198r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0390

Rule Title: The HPBPW Control Option is not set to (3) days maximum.

Vulnerability Discussion: The HPBPW Control Option selects the maximum number

of days that TSS will honor an expired or previous password for batch jobs.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0390)

b) If the HPBPW Control Option value is set to (3) days maximum, there is NO FINDING.

c) If the HPBPW Control Option value is set to greater than (3) days, this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the HPBPW control option setting to a maximum of (3) days.

CCI: CCI-000366

Group ID (Vulid): V-199

Group Title: TSS0400

Rule ID: SV-199r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0400

Rule Title: The INACTIVE Control Option must be properly set.

Vulnerability Discussion: The INACTIVE Control Option selects the number of days before TSS will deny an unused ACID access to the system after that ACIDs

password has expired. There must be no access allowed after password expiration. Suspension for inactivity should be handled using ACP00310. 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 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 migration process or contingency plan activation.

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0400)

If the INACTIVE Control Option is set to a value of "0" this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the INACTIVE Control Option to a value of "0" days and proceed with the change.

The INACTIVE Control Option value is set properly with the command:

TSS MODIFY INACTIVE(0)

CCI: CCI-000017

Group ID (Vulid): V-200

Group Title: TSS0410

Rule ID: SV-200r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0410

Rule Title: The INSTDATA Control Option is not set to (0).

Vulnerability Discussion: The INSTDATA Control Option controls the value of the 4-byte global data installation data area. This value is passed to the security

exit developed at a particular site.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(TSSPRMFL)

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(TSS0410)

b) If the INSTDATA Control Option is set to (0), there is NO FINDING.

c) If the INSTDATA Control Option is set to a value other than (0), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the INSTDATA control option value to (0) and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-201

Group Title: TSS0420

Rule ID: SV-201r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0420

Rule Title: The IOTRACE Control option must be set to (OFF).

Vulnerability Discussion: The IOTRACE Control Option controls a diagnostic trace for use by technical support. The trace is produced on the TRACE/LOG data set.

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 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 migration process or contingency plan activation.

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis requires Additional Analysis.

Automated Analysis

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

- PDI(TSS0420)

b) If the IOTRACE Control Option is set to (OFF), there is NO FINDING.

c) If the IOTRACE Control Option is not set to (OFF), this is a FINDING.

NOTE: May be set (ON) temporarily as directed by CA Technical Support for problem resolution.

Fix Text: The IAO will ensure IOTRACE control option is set to (OFF). The IOTRACE Control Option controls a diagnostic trace for use by technical support. The trace is produced on the TRACE/LOG data set.

CCI: CCI-000366

Group ID (Vulid): V-203

Group Title: TSS0440

Rule ID: SV-203r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0440

Rule Title: The LOG Control Option is not set to (SMF,INIT, SEC9, MSG). .

Vulnerability Discussion: The LOG Control Option identifies the types of events that TSS will log, and specifies whether the events will be logged onto the audit tracking file and into the SMF files. This option also specifies if the

violation message will be displayed.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0440)

b) If the LOG Control Option is set to (SMF,INIT, SEC9, MSG), there is NO FINDING.

c) If the LOG Control Option is NOT set to (SMF,INIT, SEC9, MSG), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified below and proceed with the change.

LOG(SMF,INIT, SEC9, MSG)

CCI: CCI-000130

CCI: CCI-002234

Group ID (Vulid): V-204

Group Title: TSS0450

Rule ID: SV-204r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0450

Rule Title: The LUUPDONCE Control Option value specified is not set to (NO).

Vulnerability Discussion: The LUUPDONCE Control Option indicates whether or not users last-used statistics are updated once a day following their first successful logon.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0450)

b) If the LUUPDONCE Control Option value is set to NO, there is NO FINDING.

c) If the LUUPDONCE Control Option value is set to YES, this is a FINDING.

Fix Text: The IAO will ensure LUUPDONCE control option is set to (NO). Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the control option setting to NO and proceed with the change.

CCI: CCI-000366

CCI: CCI-002251

Group ID (Vulid): V-205

Group Title: TSS0460

Rule ID: SV-205r3_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0460

Rule Title: The MODE Control Option must be set to (FAIL).

Vulnerability Discussion: The MODE Control Option selects the security mode in which TSS will operate for all facilities.

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 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 migration process or contingency plan activation.

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis requires Additional Analysis.

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

- PDI(TSS0460)

b) If the global MODE Control Option value is set to FAIL, there is NO FINDING.

c) If the global MODE Control Option value is not set to FAIL, this is a FINDING. Additional analysis may be required under the following conditions:

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

Control Options: MODE (DORMANT)
MODE (WARN)

2) Example of a possible Category I FINDING requiring additional analysis:

Control Options: MODE (IMPL)

MODE(IMPL) allows access to a data set and resource only when it is not defined to TSS. Therefore if all sensitive data sets and resources are properly defined to the security database, MODE(IMPL) will not allow unauthorized access.

Fix Text: Evaluate the impact associated with implementation of the control

option. Develop a plan of action to set the MODE control option to (FAIL) and proceed with the change.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-206
Group Title: TSS0470
Rule ID: SV-206r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0470
Rule Title: The MSUSPEND Control Option is not set to (YES).

Vulnerability Discussion: The MSUSPEND Control Option allows the MSCA ACID to be suspended automatically if the password violation threshold is set via the PTHRESH option and that limit is exceeded. This will prevent a user from making an unlimited number of guess attempts to determine the MSCAs password.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0470)

b) If the MSUSPEND Control Option is set to (YES), there is NO FINDING.

c) If the MSUSPEND Control Option is NOT set to (YES), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the MSUSPEND control option to (YES) and proceed with the change.

CCI: CCI-002361

Group ID (Vulid): V-207
Group Title: TSS0480
Rule ID: SV-207r3_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0480
Rule Title: NEWPW Control Options must be properly set.

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, 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.

The NEWPW Control Option specifies the rules that TSS will apply when a user selects a new password. Improper setting of any of these fields, individually or in combination with another, can result in weakened passwords and compromise the security of the processing environment.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0480)

If the NEWPW Control Option values conform to the following requirements, this is not a finding.

NEWPW(MIN=8,WARN=10, MINDAYS=1, NR=0, ID, TS, SC, RS, FA, FN, MC, UC, LC)

NOTE: For the Option SC, the PASSCHAR control option should be set to the

allowable list defined in CA Top Secret for z/OS Control Options Guide.

NOTE: For the Option RS, at a minimum use the reserved word prefix list found in the Addendum section 5.1.3.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified and proceed with the change.

(Support of mixed case passwords can only be set when the security file has been copied by TSSXTEND with the option NEWPWBLOCK.)

Ensure the NEWPW Control Option values conform to the following requirements:

NEWPW(MIN=8,WARN=10, MINDAYS=1, NR=0, ID, TS, SC, RS, FA, FN, MC, UC, LC)

NOTE: For the Option SC, the PASSCHAR control option should be set to the allowable list defined in CA Top Secret for z/OS Control Options Guide.

NOTE: For the Option RS, at a minimum use the reserved word prefix list found in the Addendum section 5.1.3.

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000198

CCI: CCI-000205

CCI: CCI-001395

CCI: CCI-001619

Rule ID: SV-93755r2_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0485

Rule Title: NIST FIPS-validated cryptography must be used to protect passwords in the security database.

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.

Check Content:

From a command input line enter:

TSS MODIFY(STATUS)

Alternately:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis:

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

- PDI(TSS0485)

If either of the following is included, this is not a finding.

AES_ENCRYPTION(Active,128)

AES_ENCRYPTION(Active,256)

Fix Text: Evaluate the impact associated with implementation of the control option.

Develop a plan of action to implement the control option as specified below:

Convert passwords/password phrases from Triple-DES encryption to 128-bit AES or 256-bit encryption by running TSSMAINT (with the AESENCRYPT option specified) and then running TSSXTEND to copy the old security file to the new security file.

Please consult CA-TSS Installation guide for more information.

Group ID (Vulid): V-208

Group Title: TSS0490

Rule ID: SV-208r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0490

Rule Title: The NJEUSER Control Option is not set to (NJESTORE).

Vulnerability Discussion: The NJEUSER Control Option is used to define a default ACID to be used for NJE store and forward nodes where no other ACID can be identified.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0490)

b) If the NJEUSR Control Option value is set to NJEUSR(NJESTORE), there is NO FINDING.

c) If the NJEUSR Control Option value is NOT set to NJEUSR(NJESTORE), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as follows and proceed with the change.

NJEUSER(NJESTORE)

CCI: CCI-002207

Group ID (Vulid): V-209

Group Title: TSS0500

Rule ID: SV-209r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0500

Rule Title: The NPWRTHRESH Control Option is not set to (02).

Vulnerability Discussion: The NPWRTHRESH Control Option sets the threshold value for the number of attempts allowed for new password reverification before complete logon sequence needs restarting.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0500)

b)) If the NPWRTHRESH Control Option value is set to NPWRTHRESH(02), there is NO FINDING

c) If the NPWRTHRESH Control Option value is NOT set to NPWRTHRESH(02), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

NPWRTHRESH(02)

CCI: CCI-000044

CCI: CCI-002696

Group ID (Vulid): V-4836

Group Title: TSS0505

Rule ID: SV-4836r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0505

Rule Title: The OPTIONS Control Option does not include option (4) at a minimum.

Vulnerability Discussion: The OPTIONS Control Option replaces optional APARs that have been applied prior to Release 5.1.

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 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 migration process or contingency plan activation.

NOTE: "TSS MODIFY" command will list OPTIONS as OPTIONALS. i.e. OPTIONALS(004,005)

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0505)

b) If the OPTIONS Control Option contains at a minimum option number (4), there is NO FINDING.

c) If the OPTIONS Control Option does NOT contain at a minimum the number (4), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

The OPTIONS Control Option must contain at a minimum option number (4).

Example TSS PARMFILE Control Option entry:
OPTIONS(4,5,6,12,14)

CCI: CCI-000366

Group ID (Vulid): V-210
Group Title: TSS0530
Rule ID: SV-210r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0530
Rule Title: The PRODUCTS Control Option is not set to (TSO/E) .

Vulnerability Discussion: The PRODUCTS Control Option allows the site to list special products that are installed on the system.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

Check appropriate section of the STIG for proper value or setting.

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0530)

b) If the PRODUCTS Control Option value is set to include TSO/E, there is

NO FINDING.

c) If the PRODUCTS Control Option value is not set to include TSO/E , this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified below and proceed with the change.

PRODUCTS(TSO/E)

****Note**** TSO/E is the DEFAULT value but should be specified for clarity.

CCI: CCI-000366

Group ID (Vulid): V-211

Group Title: TSS0540

Rule ID: SV-211r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0540

Rule Title: The PTHRESH Control Option is not set to (2).

Vulnerability Discussion: The PTHRESH Control Option selects a maximum password violation threshold. If the user exceeds the specified threshold by entering the wrong password too many times, TSS suspends the ACID.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0540)

b) If the PTHRESH Control Option value is set to PTHRESH(2), there is NO FINDING.

c) If the PTHRESH Control Option value is NOT set to PTHRESH(2), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

PTHRESH(2)

CCI: CCI-000044

CCI: CCI-002238

CCI: CCI-002361

Group ID (Vulid): V-212
Group Title: TSS0550
Rule ID: SV-212r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0550
Rule Title: The PWEXP Control Option is not set to (60).

Vulnerability Discussion: The PWEXP Control Option allows the site to specify a password expiration interval.

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 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 migration process or contingency plan activation.

IACControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0550)

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

b) If the PWEXP Control Option value is set to PWEXP(60), there is NO FINDING.

c) If the PWEXP Control Option value is NOT set to PWEXP(60), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the following control option setting as specified and proceed with the change.

PWEXP(60)

CCI: CCI-000199

Group ID (Vulid): V-213

Group Title: TSS0560

Rule ID: SV-213r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0560

Rule Title: The PWHIST Control Option is not set to (10) or greater.

Vulnerability Discussion: The purpose of the password history is to prevent users from reusing old passwords when their current one expires.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0560)

b) If the PWHIST Control Option value is set to PWHIST(10) or greater, there is NO FINDING.

c) If the PWHIST Control Option value is NOT set to PWHIST(10) or greater, this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the following control option setting as specified and proceed with the change.

PWHIST(10) or greater

CCI: CCI-000200

Group ID (Vulid): V-215

Group Title: TSS0580

Rule ID: SV-215r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0580

Rule Title: The RECOVER Control Option is not set to (ON).

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0580)

b) If the RECOVER Control Option value is set to RECOVER(ON), there is NO FINDING.

c) If the RECOVER Control Option value is NOT set to RECOVER(ON), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the following control option setting as specified and proceed with the change.

RECOVER(ON)

CCI: CCI-000366

CCI: CCI-002357

Group ID (Vulid): V-216

Group Title: TSS0590

Rule ID: SV-216r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0590

Rule Title: The SECTRACE Control Option is not set to (OFF).

Vulnerability Discussion: The SECTRACE Control Option activates a diagnostic security trace on the activities of all defined users.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0590)

b) If the SECTRACE Control Option value is set to SECTRACE(OFF), there is NO FINDING.

c) If the SECTRACE Control Option value is NOT set to SECTRACE(OFF), this is a Finding

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to SECTRACE(OFF) and proceed with the change.

CCI: CCI-000366

CCI: CCI-002884

Group ID (Vulid): V-217

Group Title: TSS0600

Rule ID: SV-217r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0600

Rule Title: The SUBACID Control Option is not set to (U,8).

Vulnerability Discussion: The SUBACID Control Option indicates how TSS will derive an ACID for batch jobs that are submitted through an online terminal, from another batch job, or from a started task.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0600)

b) If the SUBACID Control Option values are set to SUBACID(U,8), there is NO FINDING.

c) If the SUBACID Control Option values are NOT set to SUBACID(U,8), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to SUBACID(U,8), and proceed with the change.

CCI: CCI-002233

Group ID (Vulid): V-219

Group Title: TSS0620

Rule ID: SV-219r2_rule

Severity: CAT III

Rule Version (STIG-ID): TSS0620

Rule Title: The SYSOUT Control Option is not set to (x,LOCAL). **Note: 'x' represents a site defined JES SYSOUT class

Vulnerability Discussion: The SYSOUT Control Option spins off a TSS diagnostic log, and specifies the SYSOUT class and destination for the log.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

****NOTE**** Replace "x" with JES SYSOUT class - at sites discretion.

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0620)

b) If the SYSOUT Control Option values are not set to SYSOUT(x,LOCAL), there is NO FINDING..

c) If the SYSOUT Control Option values is not set to SYSOUT(x,LOCAL), this is a FINDING.

Fix Text: ****NOTE**** Replace "x" with JES SYSOUT class - at sites discretion. Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to SYSOUT(x,LOCAL), and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-220

Group Title: TSS0630

Rule ID: SV-220r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0630

Rule Title: The TAPE Control Option is not set to (OFF).

Vulnerability Discussion: The TAPE Control Option specifies the type of tape protection in effect at the installation.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0630)

b) If the TAPE Control Option value is set to TAPE(OFF), there is NO FINDING.

c)) If the TAPE Control Option value is NOT set to TAPE(OFF), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to TAPE(OFF), and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-221

Group Title: TSS0640

Rule ID: SV-221r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0640

Rule Title: The TEMPDS Control Option is not set to (YES).

Vulnerability Discussion: The TEMPDS Control Option allows an installation to determine whether or not temporary data sets will be protected.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0640)

b) If the TEMPDS Control Option value is set to TEMPDS(YES), there is NO FINDING.

c) If the TEMPDS Control Option value is NOT set to TEMPDS(YES), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to TEMPDS(YES), and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-222

Group Title: TSS0650

Rule ID: SV-222r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0650

Rule Title: The TIMER Control Option is not set to (30).

Vulnerability Discussion: The TIMER Control Option controls the interval at which data is written from TSS buffers to the audit tracking file.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the TSS Data Collectio

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0650)

b) If the TIMER Control Option value is set to TIMER(30), there is NO FINDING.

c) If the TIMER Control Option value is NOT set to TIMER(30), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to TIMER(30), and proceed with the change.

CCI: CCI-000174

Group ID (Vulid): V-36849

Group Title: TSS0660

Rule ID: SV-48610r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0660

Rule Title: NEWPHRASE and PPSCHAR Control Options must be properly set.

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 NEWPHRASE and PPSCHAR Control Options specify the rules that TSS 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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0660)

If the following guidance is true, this is not a finding.

____ The NEWPHRASE Control Option will conform to the following requirements.

MA=1-32

MN=1-32

ID

MAX=100

MIN=15-100

MINDAYS=1

NR=0-1

SC=1-32

WARN=1-10

____ The PPSCHAR Control Option will conform to the allowable list defined in CA Top Secret for z/OS Control Options Guide.

Note: These characters will be specified at a minimum. '40' represents the blank character. Characters can be identified by their character or hex equivalent.

Fix Text: Ensure that the NEWPHRASE and PPSCHAR Control Options values are set to the values specified.

(Support of mixed case passwords can only be set when the security file has been copied by TSSXTEND with the option NEWPWBLOCK)

Configure the NEWPHRASE Control Option values to the following requirements:

MA=1-32
MN=1-32
ID
MAX=100
MIN=15-100
MINDAYS=1
NR=0-1
SC=1-32
WARN=1-10

Configure the PPSCHAR Control Option to the allowable list defined in CA Top Secret for z/OS User Guide.

Note: These characters will be specified at a minimum. '40' represents the blank character. Characters can be identified by their character or hex equivalent.

Example:

```
TSS MODIFY NEWPHRASE(MA=1,MN=1,ID,MAX=100,MIN=15,MINDAYS=1,NR=1,SC=1,WARN=10)
TSS MODIFY PPSCHAR(c,c,c,c,...)
```

(Use the allowable list defined in CA Top Secret for z/OS Control Options Guide.)

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-36851

Group Title: TSS0670

Rule ID: SV-48612r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0670

Rule Title: NPPTHRESH Control Option will be properly set.

Vulnerability Discussion: The NPPTHRESH Control Option sets the threshold value for the number of attempts allowed for new password re-verification before complete logon sequence needs restarting.

In accordance with DODI 8500.2 for DOD information systems processing sensitive information and above, and CJCSM 6510.01, the following recommendations concerning password requirements are mandatory and apply equally to both classified and unclassified systems:

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0670)

The NPPTHRESH Control Option will conform to the following requirements. If the following guidance is true, this is not a finding.

NPPTHRESH(02)

Fix Text: The IAO will ensure that the NPPTHRESH Control Option values are set to the values specified.

Ensure the NPPTHRESH Control Option value conforms to the following requirements:

NPPTHRESH(02)

Example:

TSS MODIFY NPPTHRESH(02)

CCI: CCI-000044

CCI: CCI-002696

Group ID (Vulid): V-36852

Group Title: TSS0680

Rule ID: SV-48613r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0680

Rule Title: PPEXP Control Option will be properly set.

Vulnerability Discussion: The PPEXP Control Option allows the site to specify a password expiration interval.

In accordance with DODI 8500.2 for DOD information systems processing sensitive information and above, and CJCSM 6510.01, the following recommendations concerning password requirements are mandatory and apply equally to both classified and unclassified systems:

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0680)

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

The PPEXP Control Option will conform to the following requirements. If the following guidance is true, this is not a finding.

PPEXP(60)

Fix Text: The IAO will ensure that the PPEXP Control Option 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 PPEXP Control Option value conforms to the following requirements.

PPEXP(60)

Example:

TSS MODIFY PPEXP(60)

CCI: CCI-000199

Group ID (Vulid): V-36853

Group Title: TSS0690

Rule ID: SV-48614r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0690

Rule Title: PPHIST Control Option will be properly set.

Vulnerability Discussion: The PPHIST is to prevent users from reusing old password phrases when their current one expires.

In accordance with DODI 8500.2 for DOD information systems processing sensitive information and above, and CJCSM 6510.01, the following recommendations concerning password requirements are mandatory and apply equally to both classified and unclassified systems:

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

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

- TSSCMD5.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0690)

The PPHIST Control Option will conform to the following requirements. If the following guidance is true, this is not a finding.

PPHIST(10-64)

Fix Text: The IAO will ensure that the PPHIST Control Option values are set to the values specified.

Ensure the PPHIST Control Option value conforms to the following requirements:

PPHIST(10-64)

Example:

TSS MODIFY PPHIST(10)

CCI: CCI-000200

Group ID (Vulid): V-223
Group Title: TSS0730
Rule ID: SV-223r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0730
Rule Title: The VTHRESH Control Option values specified are not set to (10,NOT,CAN).

Vulnerability Discussion: The VTHRESH Control Option selects an access violation threshold for users, batch jobs and started tasks, and selects the action that TSS will take when the threshold is reached.

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 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 migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(TSS0730)

b) If the VTHRESH Control Option values are set to VTHRESH(10,NOT,CAN), there is NO FINDING.

c) If the VTHRESH Control Option values are not set to VTHRESH(10,NOT,CAN), this is a FINDING.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to VTHRESH(10,NOT,CAN), and proceed with the change.

CCI: CCI-002361

Group ID (Vulid): V-224

Group Title: TSS0740

Rule ID: SV-224r2_rule

Severity: CAT III

Rule Version (STIG-ID): TSS0740

Rule Title: User ACIDs and Control ACIDs do not have the NAME field completed.

Vulnerability Discussion: Every User ACID should be assigned to an individual using the name field. Within the ACID record, the users NAME field should be completed. If this field is not completed for each user, user accountability will become lost.

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

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

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)

Automated Analysis

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

- PDI(TSS0740)

Note: An interactive user may have more than one ACID as long as it has a matching DD2875 form. Users may not share any type of ACID.

b) If all ACIDs have the NAME field completed, there is NO FINDING.

c) If any ACID does not have the NAME field completed, this is a FINDING.

Fix Text: The IAO will review all ACID definitions and ensure the NAME field is completed. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement.

NOTE:

An interactive user may have more than one ACID as long as it has a matching DD2875 form. Users may not share any type of ACID.

CCI: CCI-000764

CCI: CCI-000804

Group ID (Vulid): V-225

Group Title: TSS0750

Rule ID: SV-225r4_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0750

Rule Title: PASSWORD(NOPW) option must not be specified for any ACID type.

Vulnerability Discussion: The PASSWORD(NOPW) option if specified, would allow access to ACIDs capability without specifying a password. This includes all ACID types (including USER, DCA, VCA, ZCA, LSCA, SCA, and MSCA) except for structure ACIDS such as: DEPARTMENT, DIVISION, ZONE, GROUP, and PROFILE. This would cause user accountability to be lost for those ACIDs and they could conceivably possess more authority than is necessary for them to do their job.

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)

Automated Analysis

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

- PDI(TSS0750)

NOTE: To evaluate the PASSWORD option NOPW, the TSSCMDS and CATJ0002 jobs must be run under the MSCA's ACID. If CATJ0002 is not submitted using the MSCA's ACID, the above PDI member will not be generated.

If PASSWORD(NOPW) is specified for any ACID types (USER, DCA, VCA, ZCA, LSCA, SCA, and MSCA), this is a finding.

Fix Text: Review definition of all ACID types (including USER, DCA, VCA, ZCA, LSCA, SCA, and MSCA) except for structure ACIDS such as: DEPARTMENT, DIVISION, ZONE, GROUP, and PROFILE to ensure that all ACIDs specify a password.

The following command is an example of how this can be corrected.

```
TSS REPLACE(user_ACID) PASSWORD(Text4Pwd,60)
```

CCI: CCI-000764

Group ID (Vulid): V-25505

Group Title: TSS0755

Rule ID: SV-31713r5_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0755

Rule Title: Interactive ACIDs defined to TSS must have the required fields completed.

Vulnerability Discussion: The required fields indicate the privileges and accesses that each user possesses. If the user is not associated with a group, user accountability is lost for that user and they could conceivably possess more authority than is necessary for them to do their job.

IAControls: IAIA-1, IAIA-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)

Automated Analysis

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

- PDI(TSS0755)

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

____ Ensure the fields and information listed below, are present for all interactive users.

FIELD DESCRIPTION VALUE

FACILITY Validated facilities to use BATCH, TSO, NCPASS, or other interactive Facility

PASSWORD logon password must have a value

INSTDATA Installation data optional

PROFILE Profile(s) optional

TSOLPROC Default TSO logon PROC optional for TSO users

TSOLACCT Default TSO logon account may be required for a fee for service.

___ Ensure that the PASSWORD interval is a value of 1 to 60 days.

___ Ensure that the NOSUSPEND attribute is not specified.

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 PASSWORD interval of 0 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 ACID definitions to ensure required information is provided. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required according to the following:

FIELD DESCRIPTION VALUE

FACILITY Validated facilities to use BATCH, TSO, NCPASS, or other interactive Facility

PASSWORD logon password must have a value

INSTDATA Installation data optional

PROFILE Profile(s) optional

TSOLPROC Default TSO logon PROC optional for TSO users

TSOLACCT Default TSO logon account may be required for a fee for service.

The PASSWORD interval for interactive user must be set to no higher than 60 days.

The NOSUSPEND attribute will not be specified for interactive users.

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 PASSWORD interval of 0 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.

TSS REP(userid) PASSWORD(Unk#own6,60)

CCI: CCI-000199

CCI: CCI-000764

CCI: CCI-000804

CCI: CCI-002119

Group ID (Vulid): V-226

Group Title: TSS0760

Rule ID: SV-226r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0760

Rule Title: Propagation control is not in use, thus allowing ACID inheritance.

Vulnerability Discussion: Batch jobs should have associated ACIDs identified to the system to designate the resources available to the job. Propagation control is used to secure special ACIDs that are not subject to automatic propagation of batch jobs. If propagation control is not used, the ACIDs authority of the subsystem is inherited. Failure to control batch job propagation could compromise the operating system environment, ACP, and customer data.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(FACLIST)
- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(WHOOPROP)

Automated Analysis

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

- PDI(TSS0760)

Review the FACLIST report to determine which Facilities are defined with both the MULTIUSER and ASUBM attributes. If no Facility is defined with both the MULTIUSER and ASUBM attributes further analysis is not needed.

For each Facility with MULTIUSER and ASUBM attribute, review the @ACIDS report to determine which ACID(s) has (have) the following:

- 1) A Master Facility of the Facility with MULTIUSER and ASUBM attribute, and,

2) The Facility of BATCH

If no ACID is defined with both the characteristics mentioned in above, further analysis is not needed.

For each ACID that has the Master Facility of the Facility with MULTIUSER and ASUBM attribute and has the Facility of BATCH, they will be defined to the PROPCNTL resource class.

Fix Text: Ensure an associated ACID exists for all batch jobs and propagation control is being used. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required.

The following Example shows the CONTROL-M STC ACID being owned to the PROPCNTL resource class:

TSS ADD(deptacid) PROPCNTL(control-m-acid)

CCI: CCI-002233

Group ID (Vulid): V-227

Group Title: TSS0770

Rule ID: SV-227r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0770

Rule Title: Scheduled production batch ACIDs must specify the BATCH Facility and the Batch Job Scheduler must be authorized to the Scheduled production batch ACID.

Vulnerability Discussion: Batch jobs should have associated ACIDs defined to the system to designate the resources available to the job. Access levels for batch jobs should be limited to those levels required to perform its established function. Failure to control batch job access authorizations could compromise the operating system environment and customer data.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)

Refer to the documentation of the processes used for submission of batch jobs via an automated process (i.e., scheduler or other sources) and each of the associated userids.

Ensure that each identified batch ACID is sourced to a specific submission

process used only for batch processing. If the following guidance is true, this is not a finding.

___ The job scheduler is cross-authorized to the batch ACIDs.

___ The Facility of BATCH is specified for each batch ACID.

___ Batch ACIDs with facilities other than BATCH should be questioned to ensure they are truly used for batch processing only, especially if a non-expiring password is used.

___ The batch ACIDS may have the NOSUSPEND attribute.

Fix Text: Ensure associated ACIDs exist for all batch jobs and documentation justifying access to system resources is maintained and filed with the IAO. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the required changes.

CCI: CCI-002233

Group ID (Vulid): V-19893

Group Title: TSS0780

Rule ID: SV-22058r2_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0780

Rule Title: Access to the TSS MODE resource class is inappropriate.

Vulnerability Discussion: Access to the resources in the MODE resource class overrides the security mode in which an Acid will operate for all facilities. Acids with permission to these resources can compromise the security of the processing environment. In addition, failure to restrict access to these resources introduces the possibility of exposure during migration process or contingency plan activation.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(WHOHMODE)

Automated Analysis

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

- PDI(TSS0780)

b) If any ACIDs is permitted a mode of DORM, WARN, or IMPL, this is FINDING.

c) If all ACIDs are permitted to mode of FAIL or do not have any permissions to the MODE resource class, there is NO FINDING.

Fix Text: The IAO will evaluate the impact associated with implementation of the removal of this access. Develop a plan of action to ensure that the ACIDs use the default MODE settings and proceed with the change.

CCI: CCI-000213

CCI: CCI-002358

Group ID (Vulid): V-228

Group Title: TSS0790

Rule ID: SV-228r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0790

Rule Title: Default ACID must be properly defined.

Vulnerability Discussion: The default ACID will be applied to any job that does not have a valid ACID associated with it. The FAIL mode ensures that access requests not conforming to the existing rule will fail. If the default ACID is allowed to successfully execute any batch job, there is a loss of accountability. Additionally, a job could modify or delete critical data and could potentially damage the system.

Check Content:

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

- TSSCMD5.RPT(#STC)

- TSSCMD5.RPT(@ACIDS)

Automated Analysis requires Additional Analysis.

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

- PDI(TSS0790)

b) Ensure the default STC has been set to FAIL. Otherwise, if a default ACID has been defined, review the accuracy of the ACID setup. The ACID should have no

access to resources and no facility access and sourced to the internal reader.

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

d) If (b) above is incorrect, this is a FINDING.

Fix Text: The IAO will ensure the default STC ACID is defined in accordance with the following restrictions. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as specified.

All STCs not defined to TSS will fail upon initiation. The following command may be used to associate all undefined STCs with a default action of FAIL:

```
TSS ADD(STC) PROCNAME(DEFAULT) ACID(FAIL)
```

If a valid requirement exists to establish a default STC, the following restrictions also apply:

- a. The IAO will maintain the written request, justification, and authorization.
- b. The STC's ACID will have no other facilities permitted to it.
- c. The STC's ACID will have a permission of DSN(*****) ACCESS(NONE).

```
TSS PERMIT(stc-acid) DSN(*****) ACCESS(NONE)
```

- d. The STC's ACID will not have any permission to the resources available to TSS.
- e. The STC's ACID will be sourced to the internal reader:

```
ADD(stc-acid) SOURCE(INTRDR)
```

- f. An entry will be made in the STC table identifying the default ACID name as follows ("stc-acid" site defined):

```
TSS ADD(STC) PROCNAME(DEFAULT) ACID(stc-acid)
```

CCI: CCI-002235

Group ID (Vulid): V-229
Group Title: TSS0810
Rule ID: SV-229r4_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0810

Rule Title: The BYPASS attribute must be limited to just trusted STCs.

Vulnerability Discussion: The BYPASS attribute permits STCs to bypass security checking. With this authority, a job or ACID could bypass all security checking, and could potentially alter or destroy critical system data.

Check Content:

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

- TSSCMD5.RPT(#STC)

Automated Analysis requires Additional Analysis.

Automated Analysis

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

- PDI(TSS0810)

Ensure that only STCs listed in the TRUSTED STARTED TASKS table, in the z/OS STIG addendum, are granted the BYPASS privilege.

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.

While the actual list may vary based on local site requirements and software configuration, the TRUSTED STARTED TASKS table, in the z/OS STIG addendum, is an approved list of started tasks that may be considered trusted started procedures and can have the BYPASS attribute specified in the start task table.

The site may exclude any STCs from the list of trusted started tasks based on local requirements. However, the addition of other started tasks to the list requires the approval of the site DAA.

Fix Text: Review the STC record for ACIDs with the BYPASS attribute. Ensure only those trusted STCs that are listed in the TRUSTED STARTED TASKS table, in the z/OS STIG addendum, have been granted this authority. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes.

Trusted STCs:

While the actual list may vary based on local site requirements and software configuration, the TRUSTED STARTED TASKS table, in the z/OS STIG addendum, is an approved list of started tasks that may be considered trusted started procedures:

CCI: CCI-000035

Group ID (Vulid): V-230

Group Title: TSS0820

Rule ID: SV-230r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0820

Rule Title: Started tasks must be properly defined to Top Secret.

Vulnerability Discussion: Started procedures have system generated job statements that do not contain the user, or password statements. To enable the started procedure to access the same protected resources that users and groups access, started procedures must have an associated USERID/ACID. If a USERID/ACID is not associated with the started procedure, the started procedure will not have access to the resources.

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

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(#STC)

Automated Analysis

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

- PDI(TSS0820)

Refer to a list of all started tasks (STCs) and associated userids with a brief description on the system.

Ensure that each Started Task ACID is properly defined. If the following guidance is true, this is not a finding.

____ All started tasks are assigned a unique user ACID or STC ACIDs will be unique per product and function if supported by vendor documentation.

___ Every ACID with the STC Facility has a corresponding entry defined in the STC record.

___ Every ACID defined in the STC record has a corresponding user ACID defined to TSS with the STC Facility.

___ All STC ACIDs will have a password generated in accordance with STIG requirements.

___ All STC ACIDs will be sourced to the internal reader (e.g., ADD(stc-acid) SOURCE(INTRDR)).

___ The STC ACIDs may have the NOSUSPEND attribute.

Fix Text: Review the STC record and all associated ACIDs. Ensure STCs and associated ACIDs are defined to the STC record. Restrict access to required resources only. Evaluate the impact of correcting the deficiency. Ensure TSS started task table record contains an entry for each Started Proc that maps the proc to a unique userid, or STC ACIDs will be unique per product and function if supported by vendor documentation. Develop a plan of action and implement the changes as specified:

All STC ACIDs will have the STC facility. An STC also may be granted the FAC(BATCH) if it requires the capability to submit batch jobs to the internal reader. It should be noted, however, that this also will allow the STC itself to be executed as a batch job.

TSS ADD(stc-acid) FACILITY(STC BATCH)

Each STC ACID will be defined with a password following the password requirement guidelines. The only exception is that these passwords will be defined as non-expiring. In addition, each STC will have its own unique password. Defining a password for started tasks prevents a user from logging onto a system with the STC ACID.

TSS REP(stc-acid) PASSWORD(xxxxxxx,0)

Ensure the OPTIONS control option specifies a value of 4 to disable password checking for STCs. Otherwise operators will be forced to supply a password when STCs are started.

All STC ACIDs will be sourced to the internal reader. This control will further protect the unauthorized use of STC ACIDs.

TSS ADD(stc-acid) SOURCE(INTRDR)

Every STC will be defined to the STC table, associated with a specific procedure, and granted minimum access.

TSS ADD(STC) PROCNAME(stc-proc) ACID(stc-acid)

Note: The STC ACIDs may have the NOSUSPEND attribute to exempt an STC ACID from suspension for excessive violations. Review the STC record and all associated ACIDs. Ensure STCs and associated ACIDs are defined to the STC record. Restrict access to required resources only. Evaluate the impact of correcting the deficiency. Ensure TSS started task table record contains an entry for each Started Proc that maps the proc to a unique userid, or STC ACIDs will be unique per product and function if supported by vendor documentation. Develop a plan of action and implement the changes as specified:

All STC ACIDs will have the STC facility. An STC also may be granted the FAC(BATCH) if it requires the capability to submit batch jobs to the internal reader. It should be noted, however, that this also will allow the STC itself to be executed as a batch job.

TSS ADD(stc-acid) FACILITY(STC BATCH)

Each STC ACID will be defined with a password following the password requirement guidelines. The only exception is that these passwords will be defined as non-expiring. In addition, each STC will have its own unique password. Defining a password for started tasks prevents a user from logging onto a system with the STC ACID.

TSS REP(stc-acid) PASSWORD(xxxxxxxx,0)

Ensure the OPTIONS control option specifies a value of 4 to disable password checking for STCs. Otherwise operators will be forced to supply a password when STCs are started.

All STC ACIDs will be sourced to the internal reader. This control will further protect the unauthorized use of STC ACIDs.

TSS ADD(stc-acid) SOURCE(INTRDR)

Every STC will be defined to the STC table, associated with a specific procedure, and granted minimum access.

TSS ADD(STC) PROCNAME(stc-proc) ACID(stc-acid)

Note: The STC ACIDs may have the NOSUSPEND attribute to exempt an STC ACID from suspension for excessive violations.

CCI: CCI-000764

Group Title: TSS0830

Rule ID: SV-231r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0830

Rule Title: Batch ACID(s) submitted through RJE and NJE is (are) not sourced.

Vulnerability Discussion: Jobs submitted through the RJE or NJE process will be sourced for submission to restrict the ACID so it can only be used from a specific remote number. This ensures that integrity is maintained. Without source restrictions, there is the potential job streams could be submitted from unauthorized locations.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)

Refer to the list of NJE/RJE batch jobs and each of the associated userids.

b) Refer to data obtained from the site installation identifying batch type ACIDs. Ensure that all static batch ACIDs (ACIDs whose passwords never change) originating from a physical reader, RJE, or NJE are sourced to those readers such as (INTRDR, N12.IR, etc) with the appropriate source Syntax.

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

d) If (b) above is incomplete, this is a FINDING.

Fix Text: Ensure that all static batch ACIDs (ACIDs whose passwords never change) originating from a physical reader, RJE, or NJE are sourced to those readers such as (INTRDR, N12.IR, etc) with the appropriate source Syntax.

Example: TSS ADD(batch-acid) SOURCE(device)

Develop a plan of action and implement the changes as specified

CCI: CCI-000764

Group ID (Vulid): V-232

Group Title: TSS0840

Rule ID: SV-232r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0840

Rule Title: DASD management ACIDs are not properly defined.

Vulnerability Discussion: DASD management ACIDs require access to backup and restore all files and volumes, and thus present a high degree of risk to the environment.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(@ACIDS)
- SENSITVE.RPT(WHOHVOL)

Refer to all documents and procedures that apply to Storage Management. Including identification of the DASD backup files and all associated storage management userids.

b) Refer to data obtained from the site installation identifying DASD maintenance ACIDs. Review selected ACIDs from data gathered for volume authorizations.

Note: SMS utilizes IBMFAC resource class permissions. If DFSMS/MVS is used to perform DASD maintenance operations, IBMFAC permissions may also be used to authorize storage maintenance operations to non-SMS-managed volumes in lieu of using VOLUME permissions.

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

d) If (b) above is incomplete, this is a FINDING.

ACIDs assigned to production storage maintenance tasks, such as DASD management, will be granted the appropriate authorizations necessary to perform their functions. Apply the following controls to storage management ACIDs:

(1) Define all batch ACIDs to the BATCH facility.

(2) Permit access to sensitive programs and utilities using program protection controls, such as the PROGRAM resource class and program pathing.
Note: As long as only authorized users are being granted access, program pathing is not required.

(3) Permit data set access for backup, recovery, and compaction using the VOLUME resource class. Depending on the storage management software, some data set level checking may be performed under certain conditions. For such instances, the appropriate data set access authorization should be granted. Refer to the vendor's product documentation for specific requirements.

Fix Text: Ensure that maintenance ACIDs are controlled through the use of the VOLUME resource class. SMS does not utilize VOLUME permissions for SMS-managed volumes. IBMFAC permissions must be used instead. If DFSMS/MVS is used to perform DASD maintenance operations, IBMFAC permissions may also be used to authorize storage maintenance operations to non-SMS-managed volumes in lieu of using VOLUME permissions.

Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as specified.

ACIDs assigned to production storage maintenance tasks, such as DASD management, will be granted the appropriate authorizations necessary to perform their functions. Apply the following controls to storage management ACIDs:

- (1) Define all batch ACIDs to the BATCH facility.
- (2) Permit access to sensitive programs and utilities using program protection controls, such as the PROGRAM resource class and program pathing.
Note: As long as only authorized users are being granted access, program pathing is not required.
- (3) Permit data set access for backup, recovery, and compaction using the VOLUME resource class. Depending on the storage management software, some data set level checking may be performed under certain conditions. For such instances, the appropriate data set access authorization should be granted. Refer to the vendor's product documentation for specific requirements.

CCI: CCI-000764

Group ID (Vulid): V-233

Group Title: TSS0850

Rule ID: SV-233r3_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0850

Rule Title: Emergency ACIDs must be properly limited and auditing resource access.

Vulnerability Discussion: All emergency ACIDs should contain information identifying the ACID to an individual. Without this, accountability could be impaired. Since these are powerful ACIDs, it is imperative that all trace I information be maintained for the user.

IACControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPTS(TSOUADS)

Refer to the list from the IAO of all emergency userids available to the site along with the associated function of each.

Note: If running Quest NC-Pass, validate in ZNCP0020 that the Emergency ACIDS are identified as part of ZNCP0020 to have the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

If at a minimum, an emergency ACID exists with the security administration attributes specified in accordance with the following requirements, this is not a finding.

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

ADMIN Authority:

ACID(ALL)

DATA(ALL)

OTRAN(ALL)

MISC1(INSTDATA,SUSPEND,TSSSIM,NOATS)

MISC2(TSO,TARGET)

MISC8(PWMMAINT,REMASUSP)

MISC9(GENERIC) FACILITY(BATCH, TSO, ROSCOE, CICS, xxxx)

Where 'xxxx' is a facility the application security team grants access into for their application users.

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

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

Data set permissions for the emergency ACIDs will be permitted as follows:

TSS PER(acid) DSN(*****) ACCESS(ALL) ACTION(AUDIT)

Security Bypass Attributes NODSNCHK, NOVOLCHK, and NORESCHK will not be given to the Emergency ACIDs.

All emergency ACID(s) are to be implemented with logging to provide an audit

trail of their activities.

All emergency ACID(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 ACID(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 ACID(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 IAO. When an emergency ACID is released for use, its password is to be reset by the IAO within 12 hours.

- 1) Review the access authorizations for all emergency ACIDs to ensure that all access permitted to these ACIDs is reviewed and approved by the IAO.
- 2) If emergency ACIDs are utilized, ensure they are restricted to performing only the operating system recovery functions or the ACP administration functions.

Fix Text: Review all emergency ACIDs and ensure access granted is limited to resources required to support the specific functions of the owning department and that access to these resources is audited. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-235
Group Title: TSS0870
Rule ID: SV-235r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0870
Rule Title: MSCA ACID will perform security administration only.

Vulnerability Discussion: Since the MSCA is a special security administrator ACID, it has unlimited administrative authority. The MSCA can create SCAs and LSCAs, scope zones, extend the security database, so it should only be utilized for this purpose.

The system MSCA will be a limited-use ACID, which is not available to any individual for day-to-day processing. Limit it's use only to performing security

administration functions. An SCA will assume the use of, and the responsibility for, the MSCA.

The MSCA account is identified in an ACID listing as the only ACID with:
TYPE = MASTER

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(@SCA)

If the MSCA ACID has access limited to performing security administration functions only, this is not a finding.

Below is an example of allowed setup for MSCA account and authorities. "MSCA" as the Accessorid, is merely an Example here, which is site determined. List is not all inclusive. The primary SCA for the domain will be listed within the "NAME" field since they are responsible for the MSCA ACID.

```
ACCESSORID = MSCA NAME = "primary SCA"
TYPE = MASTER
FACILITY = BATCH
PROFILES = SECURID
ATTRIBUTES = AUDIT,CONSOLE,NOATS
DATASET = %. *.
DATASET = ***** +.
VOLUMES = *(G)
XA DATASET = SYS3.TSS.BACKUP
ACCESS = UPDATE
ACTION = AUDIT
----- ADMINISTRATION AUTHORITIES
RESOURCE = *ALL*
ACCESS = ALL
ACID = *ALL*
FACILITIES = *ALL*
LIST DATA = *ALL*,PROFILES,PASSWORD,SESSKEY
MISC1 = *ALL*
MISC2 = *ALL*
MISC4 = *ALL*
MISC8 = *ALL*
MISC9 = *ALL*
```

NOTE 1: Update access to the backup security database is required by the MSCA account anytime the IAO needs to run/submit the TSS Utility called TSSFAR. MSCA account may from time to time be required to have additional access for the period of project such as Extending the Security Database.

NOTE 2: MSCA account shall be used for such items as: TSSFAR, EXTENDING Security Database, creating SCA/LSCA accounts, working with LSCA accounts (scoping, admin rights, etc). Most often the IAO staff shall utilize their normal SCA account. The MSCA account shall not be anyone's primary security administrative account.

NOTE 3: MSCA account shall be limited in access, to least privileged access of resources required to function.

NOTE 4: If running Quest NC-Pass, validate in ZNCP0020 that the MSCA ACID has the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

Fix Text: The IAO will review the MSCA and ensure access granted is limited to those resources necessary to support the security administration function. Evaluate the impact of correcting the deficiency and develop a plan of action to implement the changes.

Below is an example of allowed setup for MSCA account and authorities. "MSCA" as the Accessorid, is merely an Example here, which is site determined. List is not all inclusive. The primary SCA for the domain will be listed within the "NAME" field since they are responsible for the MSCA ACID.

```
ACCESSORID = MSCA NAME = "primary SCA"
TYPE = MASTER
FACILITY = BATCH
PROFILES = SECURID
ATTRIBUTES = AUDIT,CONSOLE,NOATS
DATASET = %. *.
DATASET = ***** +.
VOLUMES = *(G)
XA DATASET = SYS3.TSS.BACKUP
ACCESS = UPDATE
ACTION = AUDIT
----- ADMINISTRATION AUTHORITIES
RESOURCE = *ALL*
ACCESS = ALL
ACID = *ALL*
FACILITIES = *ALL*
LIST DATA = *ALL*,PROFILES,PASSWORD,SESSKEY
MISC1 = *ALL*
MISC2 = *ALL*
MISC4 = *ALL*
MISC8 = *ALL*
MISC9 = *ALL*
```

NOTE 1: Update access to the backup security database is required by the MSCA account anytime the IAO needs to run/submit the TSS Utility called TSSFAR.

MSCA account may from time to time be required to have additional access for the period of project such as Extending the Security Database.

NOTE 2: MSCA account shall be used for such items as: TSSFAR, EXTENDING Security Database, creating SCA/LSCA accounts, working with LSCA accounts (scoping, admin rights, etc). Most often the IAO staff shall utilize their normal SCA account. The MSCA account shall not be anyone's primary security administrative account.

NOTE 3: MSCA account shall be limited in access, to least privileged access of resources required to function.

NOTE 4: If running Quest NC-Pass, validate in ZNCP0020 that the MSCA ACID has the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

CCI: CCI-000035

CCI: CCI-002235

Group ID (Vulid): V-236

Group Title: TSS0880

Rule ID: SV-236r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0880

Rule Title: Password changes to the MSCA ACID will be documented in the change log.

Vulnerability Discussion: The system MSCA will be a limited use ACID, which is not available to any individual for day to day processing. Limit its use only to performing required security administration functions. The Primary SCA will assume the use of, and the responsibility for, the MSCA by changing the MSCA password. The password change command will include a comment indicating the reason.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCHNGS.RPT

Note: If running Quest NC-Pass, validate in ZNCP0020 that the MSCA ACID has the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

If the MSCA password changes are documented in the change log, this is not a finding.

Fix Text: The IAO will ensure that the MSCA password changes are documented with comments in the the TSS Recovery file. The TSS Recovery file will be of sufficient size to ensure that the change is documented.

CCI: CCI-001403

CCI: CCI-002234

Group ID (Vulid): V-237

Group Title: TSS0890

Rule ID: SV-237r3_rule

Severity: CAT I

Rule Version (STIG-ID): TSS0890

Rule Title: ACIDs granted the CONSOLE attribute must be justified.

Vulnerability Discussion: CONSOLE attribute grants the ability to modify SECURITY PRODUCT CONTROL options online, including capability to change many critical Control Options. Restricting this facility prevents operators or other personnel from executing sensitive started tasks or changing security control options without proper authorization.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSPRIV.RPT

Automated Analysis

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

- PDI(TSS0890)

Ensure that ACIDs with CONSOLE authority are limited to authorized SCA security administrators and the system programmers that maintain the CA-TSS software product only.

Fix Text: Review all ACIDs with the CONSOLE attribute. Ensure access is limited to authorized SCA security administrators only. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes. Ensure documentation providing justification for access is maintained and filed with the IAO.

CCI: CCI-000035

Group ID (Vulid): V-238

Group Title: TSS0900

Rule ID: SV-238r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0900

Rule Title: ACIDs defined as security administrators do not have the attribute of NOATS.

Vulnerability Discussion: NOATS prevents the TSS administrator ACID from signing on through automatic terminal signon. If an ACID has ATS enabled, a terminal could be automatically assigned that ACID without a user being present. This applies to CICS, IMS, and IDMS.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(@ALL)
- TSSPRIV.RPT

Automated Analysis

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

- PDI(TSS0900)

Review all security administrators to ensure that each one has the NOATS attribute.

Fix Text: Review all security administrator ACIDs. Ensure the NOATS attribute has been assigned. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes.

NOTE:

The NOATS attribute may be added to an ACID or an ACID's PROFILE.

The following command may be issued to determine if the NOATS attribute is defined to an ACID or an ACID's PROFILE:

tss list(<acid>) data(basic,profile)

CCI: CCI-000035

Group ID (Vulid): V-239
Group Title: TSS0910
Rule ID: SV-239r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0910
Rule Title: Number of control ACIDs is not justified and properly assigned.

Vulnerability Discussion: Since the control ACIDs are the security administrators and can execute security modification commands, it is important that this level of access be restricted to a limited number of ACIDs. The fewer control ACIDs that there are, the more accountability and control there is over the security database.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(@SCA)

b) TYPE=CENTRAL, TYPE=MASTER or also known as "SCA" and "MSCA" level of ACIDS shall adhere to the following restrictions based upon documented role/function an individual performs:

- 1) Domain level Information Assurance Officer (IAO) – full administrative authorities and access rights needed to perform required and documented role/responsibilities/function.
- 2) Assistance Domain Level Information Assurance Officer or "backup" or IAO (up to same access as b.1).
- 3) DISA FSO SRR Auditor, DoD IG Auditor, SAS70 Auditor – only "view" administrative authorities shall be granted and only for those roles/functions that have been formally documented as DISA, DoD IG or SAS70 Auditors and approved by the DISA DAA for those position/functions/roles.

Exception: Until scoping is worked out and resolved, DISA OST team members may be defined as TYPE=CENTRAL with limited authority such as ACID(INFO,MAINTAIN). All OST Team member ACIDS shall be changed to TYPE=LIMITED and scoped accordingly to allow password resets upon verification of users, yet to limit and eliminate any potential risk associated with resetting of MSCA or other SCA level accounts. NO Other exceptions shall exist.

c) Determine if TYPE=CENTRAL and TYPE=MASTER are assigned accordingly to (b.1) – (b.3) above.

d) If all are assigned according to (b.1) – (b.3) there is NO FINDING.

e) If any are NOT assigned according to (b.1) – (b.3), there is a FINDING.

Fix Text: Review all security administrator ACIDs. Evaluate the impact of correcting the deficiency. Develop a plan of action and reduce the number of control ACIDs if not justified. Use information below as guidance.

TYPE=CENTRAL, TYPE=MASTER or also known as “SCA” and “MSCA” level of ACIDS shall adhere to the following restrictions based upon documented role/function an individual performs:

- 1) Domain level Information Assurance Officer (IAO) – full administrative authorities and access rights needed to perform required and documented role/responsibilities/function.
- 2) Assistance Domain Level Information Assurance Officer or “backup” or IAO (up to same access as 1).
- 3) DISA FSO SRR Auditor, DoD IG Auditor, SAS70 Auditor – only “view” administrative authorities shall be granted and only for those roles/functions that have been formally documented as DISA, DoD IG or SAS70 Auditors and approved by the DISA DAA for those position/functions/roles.

Exception: Until scoping is worked out and resolved, DISA OST team members may be defined as TYPE=CENTRAL with limited authority such as ACID(INFO,MAINTAIN). All OST Team member ACIDS shall be changed to TYPE=LIMITED and scoped accordingly to allow password resets upon verification of users, yet to limit and eliminate any potential risk associated with resetting of MSCA or other SCA level accounts. NO Other exceptions shall exist.

CCI: CCI-001559

CCI: CCI-002145

Group ID (Vulid): V-240
Group Title: TSS0920
Rule ID: SV-240r3_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0920
Rule Title: Security control ACIDs must be limited to the administrative authorities authorized and that require these privileges to perform their job duties.

Vulnerability Discussion: Since control ACIDs possess a significant amount of power, it is important to limit the number of control ACIDs. These ACIDs can perform and control security administration. An ACID who possesses control over

security administration could alter or modify any data set, and delete any audit trail that might have existed for the file.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(@ADMIN)

b) Determine if any ACIDs other than TYPE=CENTRAL (SCA/MSCA) has the following administrative authority:

FACILITIES(ALL)
PROGRAM(ALL)
PROGRAM(OWN)
RESOURCE(ALL)
ROSRES(ALL)
VOLUME(ALL)
VOLUME(OWN)

MISC1(ALL)
MISC1(LCF)
MISC1(LTIME)
MISC1(RDT)
MISC1(USER)

MISC2(ALL)
MISC2(DLF)
MISC2(NDT)
MISC2(SMS)

MISC4(ALL)

MISC8(ALL)
MISC8(LISTAPLU)
MISC8(LISTRDT)
MISC8(LISTSDT)
MISC8(LISTSTC)
MISC8(MCS)

MISC9(ALL)
MISC9(BYPASS)
MISC9(CONSOLE)
MISC9(GLOBAL)
MISC9(MASTFAC)
MISC9(MODE)
MISC9(STC)

MISC9(TRACE)

Additionally, decentralized security administrators shall not have scope/control over DISA internal system/domain level resources.

c) The following are “approved” Examples for other types (DCA, VCA, ZCA, LSCA) that require administrative authorities: (note: these are examples and does not mean everyone should have all of these levels).

 DATASET(ALL)ACC(ALL)
 DATASET(XAUTH,OWN,REPORT,AUDIT,INFO)ACC(ALL)
 OTRAN(ALL)ACC(ALL)
 ACID(ALL)
 ACID(INFO,MAINTAIN)
 MISC1(INSTDATA,SUSPEND,TSSSIM,NOATS)
 MISC2(TSO,TARGET)
 MISC8(PWMAINT,REMASUSP)

MISC9(GENERIC)

FACILITY(BATCH, TSO, ROSCOE, CICS, xxxx)

Where ‘xxxx’ is a facility the application security team grants access into for their application users. This shall not be STC, CA1, DFHSM or other “domain level mastfac/facility. This is only for those “onlines” that users truly log into to access their applications/data such as TSO, CICS regions, IDMS, ROSCOE, FTP, etc.

TSS ADMIN(acid)RESOURCE(REPORT,INFO,AUDIT) can be allowed and is required to run TSSUTIL reports.

Note: “RESOURCE” can specify a more specific Resource Class, such as “OTRAN”, “DATASET”, “IDMSGON”, “PROGRAM” for non SCA/MSCA type of accounts. These administrators will not have “RESOURCE” specified in administrative authority.

Note: “ALL” will display as “*ALL*” but also means approved for any single administrative authority under that specific item.

d) If no item in (b) above is found on any TYPE=DCA, VCA, ZCA, LSCA, USER, PROFILE, there is NO FINDING.

e) If any item in (b) above is found on TYPE=DCA, VCA, ZCA, LSCA, USER, PROFILE, this is a FINDING.

Fix Text: Review all security administrator ACIDs. Evaluate the impact of limiting the amount of excessive administrative authorities. Develop a plan of action and implement the changes.

CCI: CCI-000035

CCI: CCI-002145

Group ID (Vulid): V-241
Group Title: TSS0930
Rule ID: SV-241r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0930
Rule Title: The number of ACIDs possessing the tape Bypass Label Processing (BLP) privilege is not limited.

Vulnerability Discussion: BLP is extremely sensitive, as it allows the circumvention of security access checking for the data. If an unauthorized user possesses BLP authority, they could potentially read any restricted tape and modify any information once it has been copied.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- SENSITVE.RPT(WHOHVOL)

b) Using the reports listed in (a) above, review the ACIDs that have BLP access. Verify that only authorized personnel have BLP access and that documentation for access is on file with the IAO.

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

d) If (b) above is incorrect, this is a FINDING.

Fix Text: Review all ACIDs with the BLP attribute. Evaluate the impact of removing BLP access from unauthorized personnel. Develop a plan of action and remove BLP access from unauthorized ACIDs.

CCI: CCI-000035

Group ID (Vulid): V-243
Group Title: TSS0950
Rule ID: SV-243r3_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0950

Rule Title: The number of ACIDs with MISC9 authority must be justified. ACIDs with MISC9 must be limited to the administrative authorities authorized and that require these privileges to perform their job duties.

Vulnerability Discussion: The MISC9 authority deals with higher level administrative authorities. One of the authorities is The MISC9 authority deals with higher level administrative authorities. One of the authorities is BYPASS, which can bypass security on the system. This violates the principle of individual user accountability. If this authority is not monitored, the potential for system degradation or destruction could happen. Only the appointed SCA's who are responsible for the security at the domain shall have MISC9 admin rights except MISC9(Generic) may be granted to any DCA,VCA,ZCA,LSCA,SCA.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(@ADMIN)

b) Review ACIDs having MISC9(ALL) or MISC9(CONSOLE) authority under administrative authorities. Only designated SCA's who are responsible for the security for the domain will be allowed this authority.

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

d) If (b) above is not in compliance, this is a FINDING.

Fix Text: Review all ACIDs with the MISC9 attribute. Evaluate the impact of removing MISC9(ALL) or MISC9(CONSOLE) access from ACIDs not required to assign the CONSOLE attribute. It is suggested that MISC9(CONSOLE) assignment privileges be limited to the MSCA. Develop a plan of action and implement the changes.

CCI: CCI-000035

CCI: CCI-002145

Group ID (Vulid): V-244
Group Title: TSS0970
Rule ID: SV-244r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0970

Rule Title: TRACE attribute has been found assigned to ACIDs.

Vulnerability Discussion: The TRACE attribute allows ACIDs to diagnose the security trace information. This information goes to the SYSLOG dataset. This could give an ACID the ability to access system control information.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSPRIV.RPT

Automated Analysis

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

- PDI(TSS0970)

Review ACIDs having the TRACE attribute. TRACE should not be assigned.

Note: The IAO will ensure that the trace attribute is only used for trouble shooting purposes.

Fix Text: Review all ACIDs with the TRACE attribute. Evaluate the impact of correcting the deficiency. Develop a plan of action and remove the TRACE attribute.

Example:

TSS REMOVE(acid) TRACE.

CCI: CCI-002883

Group ID (Vulid): V-245

Group Title: TSS0980

Rule ID: SV-245r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0980

Rule Title: Documentation confirming the necessity of NO***CHK attributes is not available.

Vulnerability Discussion: Because the NO***CHK attributes can bypass system security, it is imperative that all ACIDS possessing these attributes be monitored and documentation maintained justifying the need for the access authorization. If these attributes are given to ACIDs that do not require the authority, the ACIDs could modify system data and potentially degrade or destroy

system information.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSPRIV.RPT

Review ACIDs having the following attributes specified. These attributes will be identified in the TSSPRIV.RPT as follows:

NDSN - NODSNCHK

NLCF - NOLCFCHK

NRES - NORESCHK

NSUB - NOSUBCHK

NVMD - NOVMDCHK

NVOL - NOVOLCHK

NOTE: NOSUBCHK attribute must be given to CICS Regions, IDMS Regions, etc. to be able to submit Jobs on behalf of all users.

This applies to ACIDs having the NOxxxCHK attributes.

Started tasks that are listed in the TRUSTED STARTED TASKS table, in the z/OS STIG Addendum are permitted to have the NOxxxCHK attributes.

Ensure that the use of the NOxxxCHK attribute is avoided unless a special requirement necessitates their use and the IAO documents all uses of the NOxxxCHK attributes.

Verify that any ACID having the NO***CHK attribute has documentation on file concerning the assignment of the attribute.

Fix Text: The IAO will ensure that the use of NOxxxCHKs is avoided unless a special requirement necessitates their use and the IAO documents all uses of NOxxxCHKs.

Review all ACIDs with the NO***CHK attribute. Evaluate the impact of correcting the deficiency. Develop a plan of action and remove the NO***CHK attribute(s).

Example:

TSS REMOVE(acid) NODSNCHK

CCI: CCI-002230

CCI: CCI-002289

Group ID (Vulid): V-246
Group Title: TSS0990
Rule ID: SV-246r2_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0990
Rule Title: ACIDs were found having access FAC(*ALL*).

Vulnerability Discussion: All users with the exception of the master security control ACID must be authorized to a facility in order to sign on to it. When a user is granted FACILITY(*ALL*) , it gives the user access to all facilities. Users should be limited to access only those facilities that are required to perform their jobs successfully.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)

Automated Analysis

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

- PDI(TSS0990)

Ensure that no ACID(s) is (are) assigned FACILITY(*ALL*).

Fix Text: The IAO will ensure that blanket access to all facilities; FACILITY(ALL), is never granted.

Review all access to FACILITY(*ALL*). Evaluate the impact of correcting the deficiency. Develop a plan of action and remove access to FAC(*ALL*).

Example:

TSS REM(acid) FAC(ALL)

CCI: CCI-000213

CCI: CCI-002230

Group ID (Vulid): V-21948
Group Title: TSS0995

Rule ID: SV-25130r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS0995

Rule Title: The TSS ALL record has inappropriate access to Facility Matrix Tables.

Vulnerability Discussion: All users with the exception of the master security control ACID must be authorized to a facility in order to sign on to it. When the ALL record is assigned Facilities, by default all users on the system have access to that Facility. Users should have limited access, only those facilities that are required to perform their jobs successfully are to be granted directly or via profile(s).

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(#ALL)
- TSSCMDS.RPT(FACLIST)

Automated Analysis

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

- PDI(TSS0995)

Review the ALL record for the assignment of FACILITY.

The IAO will ensure that with the exception of DFHSM/HSM, Top Secret facilities will not be granted via the ALL record. The DFHSM/HSM FACILITY can be determined by reviewing FACLIST for the FACILITY that contains INITPGM=ARC.

Fix Text: Review ALL record for FACILITY access. Evaluate the impact of correcting the deficiency. Develop a plan of action and remove access.

CCI: CCI-000213

Group ID (Vulid): V-22

Group Title: TSS1000

Rule ID: SV-22r2_rule

Severity: CAT II

Rule Version (STIG-ID): TSS1000

Rule Title: Dataset masking characters are not properly defined to the security database.

Vulnerability Discussion: TSS provides masking as an additional method for reducing the number of entries that must be made to secure the installation data sets. Shared patterns can be used as the operands of data set parameters. If these characters are not defined to the database, each data set name or resource must be specifically entered into the database. This additional workload for security administrator presents the increased possibility of exposure when granting access to data sets.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(WHOODSN)

Automated Analysis

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

- PDI(TSS1000)

b) Review ownership of all dataset masking characters. (*, %, and +)

c) If dataset masking characters are owned by the MSCA, there is NO FINDING.

d) If all dataset masking characters are defined, there is NO FINDING.

e) If any of the above is untrue, this is a FINDING.

Fix Text: The IAO will ensure that the MSCA owns all dataset masking characters.

Review the resource definitions for dataset masking characters ensuring they are defined to the security database. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the required changes.

Example TSS commands to protect masking characters:

TSS ADD(msca) DSN(*)

TSS ADD(msca) DSN(%)

TSS ADD(msca) DSN(+)

CCI: CCI-000213

CCI: CCI-002357

Group ID (Vulid): V-22648

Group Title: TSS1010

Rule ID: SV-26592r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS1010

Rule Title: Data set masking characters allowing access to all data sets must be properly restricted in the security database.

Vulnerability Discussion: TSS provides masking as an additional method for reducing the number of entries that must be made to secure the installation data sets. Shared patterns can be used as the operands of data set parameters. If this masking character (*, *., and/or **) are not restricted, there is the possibility of exposure when granting access to the data set mask allowing access to all data sets. Unauthorized access could result in the compromise of the operating system environment, ACP, products, and customer data.

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

Check Content:

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

- SENSITIVE.RPT(GLOBRPT)

Automated Analysis

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

- PDI(TSS1010)

Verify that the accesses to the TSS masking character (*, *., and/or **) for data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS data set access authorizations restricts READ access to auditors.

___ The TSS data set access authorizations restricts READ and/or greater access to DASD administrators, Trusted Started Tasks, emergency users, and DASD batch users.

___ If CA VTape is installed on the systems, the TSS data set access authorizations restricts READ access to CA VTape STCs and/or batch users.

___ The TSS data set access authorizations specify that all (i.e., failures and successes) EXECUTE and/or greater accesses are logged.

Fix Text: The IAO will review access authorization to the TSS mask character (*, *, and/or **) for data sets. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to restrict access to the data set mask permissions.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have WRITE and/or greater access and, if required, that all WRITE and/or greater accesses are logged. He will identify if any additional groups have WRITE and/or greater access for specific data sets, and once documented he will work with the IAO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

(Note: The data sets and/or data set prefixes identified below are examples of a possible installation. The actual data sets and/or prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Auditors may require READ access to all data sets.

DASD administrators, Trusted Started Tasks, emergency users, and DASD batch users that require READ and/or greater access to perform maintenance to all data sets.

If CA VTape is installed on the system, READ access can be given to the CA VTape STCs and/or batch users.

All accesses authorizations will be logged, the exception is the logging requirement is not required for Trusted Started Tasks.

The following commands are provided as a sample for implementing data set controls:

```
TSS ADDTO(msca) DATASET(*.)  
TSS PERMIT(audtaut) DATASET(*.) ACCESS(READ) ACTION(AUDIT)  
TSS PERMIT(CA VTape STC) DATASET(*.) ACCESS(READ) ACTION(AUDIT)  
TSS PERMIT(dasbaudt) DATASET(*.) ACCESS(ALL) ACTION(AUDIT)  
TSS PERMIT(dasdaudt) DATASET(*.) ACCESS(ALL) ACTION(AUDIT)  
TSS PERMIT(emeraudt) DATASET(*.) ACCESS(ALL) ACTION(AUDIT)  
TSS PERMIT(tstcaudt) DATASET(*.) ACCESS(ALL)
```

CCI: CCI-000213

Group ID (Vulid): V-247

Group Title: TSS1030

Rule ID: SV-247r3_rule

Severity: CAT I

Rule Version (STIG-ID): TSS1030

Rule Title: Volume access greater than CREATE found in CA-Top Secret (TSS) database must be limited to authorized information technology personnel requiring access to perform their job duties.

Vulnerability Discussion: Access authorization to data sets is verified by examining both volume access and data set access authorization. If a user has been authorized for any volume access greater than CREATE, then TSS allows access to the volume without checking the data set authorizations. A user could potentially alter a data set that resides on a volume even though access has not been granted to that data set.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- SENSITVE.RPT(WHOHVOL)

b) Determine whether or not access authorization greater than CREATE (e.g. CONTROL or ALL) has been granted for volumes.

c) If access authorizations for volumes are within the requirements, there is NO FINDING.

d) If access authorization for volumes exceeds the requirements without justification, this is a FINDING.

NOTE: Domain level DASD Administrators who are responsible for the Domain level DASD/storage administration. Volume level access to those team members who are directly responsible and perform Domain level DASD/Storage administration may be granted access to all volumes via PRIVPGM controls.

Fix Text: The IAO will ensure that VOLUME access authorization greater than CREATE is not permitted unless authorized by the IAO.

Review all access to VOLUMES. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the required changes.

*Noted Exception: Domain level DASD Administrators who are responsible for the Domain level DASD/storage administration. Volume level access to those team members who are directly responsible and perform Domain level DASD/Storage administration may be granted access to all volumes via PRIVPGM controls.

Domain Level DASD/Storage administrators access should be granted
VOL(*ALL*)ACC(ALL)ACTION(AUDIT)PRIVPGM(list of privileged programs)

CCI: CCI-000213

Group ID (Vulid): V-248

Group Title: TSS1040

Rule ID: SV-248r3_rule

Severity: CAT II

Rule Version (STIG-ID): TSS1040

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.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- SENSITVE.RPT(TSS1040)

Automated Analysis

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

- PDI(TSS1040)

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 TSS resources are owned or DEFPROT is specified for the resource class.

___ The TSS resource access authorizations restrict access to the appropriate personnel.

___ The TSS 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 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 TSS resources as designated in the above table are owned and/or DEFPROT is specified for the resource class.

The TSS 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:

TSS ADD(dept-acid) PROGRAM(AHLGTF)
TSS PERMIT(stcgaudt) PROGRAM(AHLGTF) ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

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.

IACControls: 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.

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-7529r2_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.

Check Content:

a) Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- TSSCMDS.RPT(WHOOOTRA)
- SENSITIVE.RPT(WHOHOTRA)

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010.

b) Ensure the following items are in effect for all CICS regions:

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.

c) If sensitive transactions referenced in (b) are protected as indicated, there is NO FINDING.

d) If any sensitive transaction referenced in (b) is not protected as indicated, this is a FINDING.

Fix Text: Develop a plan to implement the required changes.

1. Most transactions are protected by profiles. An example would be "L2TRANS" which would be permitted all Category 2 transactions. L2TRANS is defined to CA-TSS as a profile and is permitted to all the Category 2 transactions. An example of how to implement this within CA-TSS is shown here:

TSS CRE(L2TRANS) TYPE(PROF) DEPT(<dept acid>) NAME('L2 TRANS') INSTDATA('PROFILE GRANTING ACCESS TO ALL CATEGORY 2 TRANS')

TSS ADD(<owning acid>) OTRAN(CADP CBAM CDBC)

TSS PER(L2TRANS) OTRAN(CADP CBAM CDBC)

Permission to the transaction group can be accomplished with a sample command:

TSS PER(USERID)OTRAN(TRANSACTION)

Permission to the transactions can be accomplished by adding the L2TRANS profile to a user's ACID.

Example:

TSS ADD(<user's acid>) PROF(L2TRANS)

2. Transactions groups should be defined and permitted in accordance with the CICS Transaction tables listed in the zOS STIG Addendum.

CCI: CCI-000213

Group ID (Vulid): V-302

Group Title: ZCIC0030

Rule ID: SV-7531r3_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.

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CICSPROC)

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

- CICS.RPT(DFHSITxx)

Refer to the information gathered from the CICS Systems Programmer's Worksheet filled out from previous vulnerability ZCIC0010.

Refer to the CICS region SYSLOG - (Alternate source of SIT parameters) be sure to process DFHSIT based on the order specified. 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=DFHSIP 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).

Ensure the following CICS System Initialization Table (SIT) parameter settings are specified for each CICS region. If the following guidance is true, this is not a finding.

____ 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 is the hex and bit settings for this flag.

X'80' EQU B'10000000' External Security Requested

____ 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 is the hex and bit settings for this flag.

X'04' EQU B'00000100' Surrogate User Checking required

____ 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.

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=DFHSIP 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 listed 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

DFTUSER=<parameter> - If DFTUSER 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 listed 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

: SNSCOPE=NONE is only allowed with test/development regions.

CCI: CCI-000366

Group ID (Vulid): V-44
Group Title: ZCIC0040
Rule ID: SV-7533r3_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.

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CICSPROC)

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

- TSSCMDS.RPT(@ACID)

- TSSCMDS.RPT(#STC)

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 ACID.

- 1) A unique ACID is associated with the CICS region.
- 2) No access to interactive online facilities (e.g., TSO) other than CICS.
- 3) CICS region ACID does not have any BYPASS privilege. EXCEPT: NOSUBCHK - REQUIRED FOR CICS REGIONS TO SUBMIT BATCH PROCESSING/JOB OF THE USER WHO IS LOGGED INTO CICS.
- 4) Ensure that each CICS region ACID is associated with a TSS CICS facility. For example:

TSS ADD(CICS region ACID) MASTFAC(CICS facility)

5) CICS region is defined in the STC table. For example:

TSS ADD(STC) PROCNAME(CICS region) ACID(CICS ACID)

c) If (b) are true, this is not a finding.

d) If (b) are untrue, this is a finding.

Fix Text: Review all CICS region, default, and end-user userids to ensure they are defined and controlled as required.

Ensure the following items are in effect for each CICS region ACID:

A unique ACID is associated with the CICS region.

No access to interactive online facilities (e.g., TSO) other than CICS.

CICS region ACID does not have any BYPASS privilege.

CICS region ACID is associated with a TSS CICS facility (The IAO will determine the MASTFAC used)

CICS region is defined in the STC table.

For example:

TSS ADD(STC) PROCNAME(CICS region) ACID(CICS ACID)

CCI: CCI-000764

Group ID (Vulid): V-7119

Group Title: ZCIC0041

Rule ID: SV-7537r3_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. 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.

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CICSPROC)

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

- TSSCMDS.RPT(@ACIDS)
- SENSITVE.RPT(WHOHOTRA)

Refer to the information gathered from the CICS Systems Programmer's Worksheet filled out from previous vulnerability ZCIC0010.

Ensure the following items are in effect for the CICS default ACID (i.e., DFLTUSER=default userid). If all of the following guidance is true, this is not a finding.

- 1) Not granted the TSS BYPASS privilege.
- 2) No access to interactive on-line facilities (e.g., TSO) other than CICS.
- 3) OPTIME parameter 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).

Fix Text: Review all CICS region, default, and end-user userids to ensure they are defined and controlled as required.

Ensure the following items are in effect for the CICS default ACID (i.e., DFLTUSER=default userid):

- 1) Not granted the TSS BYPASS privilege.
- 2) No access to interactive on-line facilities (e.g., TSO) other than CICS.
- 3) OPTIME parameter is set to 15 minutes. can be increased up to 30 if justified by the IAM.
- 4) 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).

CCI: CCI-000764

Group ID (Vulid): V-7120

Group Title: ZCIC0042

Rule ID: SV-7543r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZCIC0042

Rule Title: CICS logonid(s) must be configured with proper timeout and signon limits.

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.

Documentable: YES

Check Content:

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

- TSSCMD5.RPT(@ACIDS)

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010.

NOTE: Note: Any ACID that does not have an OPTIME value specified will obtain its OPTIME value from the default value set in ZCIC0041. Any ACID that specifies an OPTIME value must meet the requirements specified below.

b) For all ACIDs authorized to access a CICS facility if the OPTIME field set to 15 minutes, 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 ISSM. 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 SIGNMULTI keyword for ACIDs is restricted test and development use this is not a finding.

Fix Text: Review all CICS region, default, and end-user userids to ensure they are defined and controlled as required.

Ensure that all ACIDs authorized to access a CICS facility have their OPTIME field set to 15 minutes.

Ensure that all ACIDs authorized to access a CICS facility restrict SIGNMULTI to test and development use.

Example:

TSS ADDTO(acid) OPTIME(hhmm)

TSS ADDTO(acid) FACILITY(facility) SIGNMULTI

CCI: CCI-000057

Group ID (Vulid): V-7121

Group Title: ZCICT041

Rule ID: SV-7525r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZCICT041

Rule Title: CICS userids are not defined and/or controlled in accordance with proper 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.

IACControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

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

- TSSCMDS.RPT(WHOOPROP)

Refer to the CICS Systems Programmer Worksheets filled out from previous vulnerability ZCIC0010.

b) Ensure the CICS region is defined to the PROPCNTL resource class.

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

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

Fix Text: Ensure the CICS region is defined to the PROPCNTL resource class.

Example:

TSS ADDTO(owning acid) PROPCNTL(CICS region acid)

CCI: CCI-000213

Group ID (Vulid): V-7555

Group Title: ZCICT050

Rule ID: SV-8032r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZCICT050

Rule Title: Control options for the Top Secret CICS facilities must meet minimum requirements.

Vulnerability Discussion: TSS CICS facilities define the security controls in effect for CICS regions. Failure to code the appropriate values could result in degraded security. This exposure may result in unauthorized access impacting the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(CICSPROC)

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

- TSSCMDS.RPT(FACLIST) - Preferred report containing all control option values in effect including default values
- TSSCMDS.RPT(TSSPRMFL) - Alternate report containing only control option values explicitly coded at TSS startup

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's facility:

- 1) The TSS CICS facility is defined with the control option values specified in the TOP SECRET INITIALIZATION PARAMETERS FOR CICS REGION Table in the z/OS STIG Addendum .

Note: An exception to the STIG is MRO CICS regions in production will use SIGN(M) appropriately.

- 2) XUSER=YES must be coded in each CICS facility.
- 3) CICS transactions defined in the BYPASS list are not sensitive transactions.

c) If the items in (b) are true for all CICS region's facility, there is NO FINDING.

d) If any item in (b) is untrue for a CICS region's facility, this is a FINDING.

Fix Text: Review the TSS control option values for all CICS facilities.
Ensure the following items are in effect for each CICS region's facility:

- 1) The TSS CICS facility is defined with the control option values specified in table - "TOP SECRET INITIALIZATION PARAMETERS FOR CICS REGION" , in the zOS STIG Addendum. Note: An exception is MRO CICS regions in production will use SIGN(M) appropriately.
- 2) XUSER=YES must be coded in each CICS facility.
- 3) CICS transactions defined in the BYPASS list are not sensitive transactions.

CCI: CCI-000366

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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Review site documentation to validate that procedures are in place to protect the FEP service subsystem and diskette drive:

- 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.

IACControls: DCCS-1, DCCS-2

Check Content:

a) Review site documentation to validate that procedures are in place to protect the FEP service subsystem and diskette drive:

- Documents and procedures restricting access to the functions of the service subsystem from the control panel.
- 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.).
- 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 (Vulid): 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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Review site documentation to validate that procedures are in place to protect the FEP service subsystem and diskette drive:

- 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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Review site documentation to validate that procedures are in place to protect the FEP service subsystem and diskette drive:

- 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 no log is in place to keep track of all hardware upgrades and software changes, this is a FINDING.

Fix Text: The systems programmer will see that 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.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- SENSITIVE.RPT(NCPRPT)

___ The ACP data set rules for NCP data sets allow inappropriate access.

___ The ACP data set rules for NCP data sets does not restrict UPDATE and/or ALL access to authorized personnel (e.g., 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: 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.

IAControls: DCCS-1, DCCS-2, IAAC-1

Check Content:

a) Review site documentation to validate that procedures are in place to protect the FEP service subsystem and diskette drive:

- 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.).

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.

c) If a key-lock switch is used to protect the modem supporting the remote console of the service subsystem, there is NO FINDING.

d) 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-6918

Group Title: ZJES0014

Rule ID: SV-7320r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZJES0014

Rule Title: RJE workstations and NJE nodes are not controlled in accordance with STIG requirements.

Vulnerability Discussion: JES2 RJE workstations and NJE nodes provide a method of sending and receiving data (e.g., jobs, job output, and commands) from remote locations. Failure to properly identify and control these remote facilities could result in unauthorized sources transmitting data to and from the operating system. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Check Content:

Remote Resource Authorizations

a) Refer to the following report produced by the OS/390 Data Collection:

- PARMLIB(JES2 parameters)

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

- TSSCMD5.RPT(WHOOIBMF)

b) Review the following resource definitions in the IBMFAC resource class:

NJE.

RJE.

NJE.nodename

RJE.workstation

NOTE 1: 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 2: Workstation is RMTnnnn, where nnnn is the number on the RMT statement. Review the JES2 parameters for RJE workstation definitions by searching for RMT(in the report.

c) If all JES2 defined NJE nodes and RJE workstations are owned in the IBMFAC class, there is NO FINDING.

NOTE: NJE. and RJE. definitions will force logonid and password protection of all NJE and RJE connections respectively. This method is acceptable in lieu of using discrete profiles.

d) If any JES2 defined NJE node or RJE workstation is not owned in the IBMFAC class, this is a FINDING.

Fix Text: Ensure associated USERIDs exist for all RJE/NJE sources and review the authorizations for these remote facilities. Develop a plan of action and implement the changes as required by the OS/390 STIG.

CCI: CCI-000213

Group ID (Vulid): V-6919

Group Title: ZJES0021

Rule ID: SV-7324r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZJES0021

Rule Title: JES2 input sources are improperly protected.

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.

Check Content:

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

- TSSCMDS.RPT(WHOOJESI)

Refer to the following report produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

b) Review the following resources in the JESINPUT resource class:

OFFn. (spool offload receiver)

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 owned.

NOTE 1: OFFn, where n is the number of the offload receiver. Review the spool offload receiver definitions by searching for OFF(in the JES2 parameters.

c) If all of the resources in (b) are owned by generic and/or fully qualified entries in the JESINPUT resource class, there is NO FINDING.

d) If any of the above resources are not owned, or are owned inappropriately, in the JESINPUT resource class, this is a FINDING.

Fix Text: Review the following resources in the JESINPUT resource class:

OFFn. (spool offload receiver)

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 owned.

NOTE 1: 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.

Ensure all of the defined resources above are owned by generic and/or fully qualified entries in the JESINPUT resource class.

For Example:

The following commands may be used to establish default protection for resources defined to the JESINPUT resource class:

TSS ADDTO(deptacid) JESINPUT(OFFn.)

Grant read access to authorized users for each of the resources defined to the JESINPUT resource class.

The following is an example of granting operators with a profile ACID of jesopracid permission to restore jobs into any SPOOL off load processor after obtaining permission from the IAO:

TSS PERMIT(jesopracid) JESINPUT(OFF*.) ACCESS(READ) ACTION(AUDIT)

The resource definition should be generic if all of the resources of the same type have identical access controls (e.g., if all off load receivers are equivalent).

CCI: CCI-000213

CCI: CCI-001310

Group ID (Vulid): V-6920

Group Title: ZJES0022

Rule ID: SV-74867r1_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.

Check Content:

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

- SENSITVE.RPT(WHOHJESI)

Verify that the accesses for JESINPUT resources are restricted. If the guidance is true, this is not a finding.

____ The TSS JESINPUT resource class in the RDT has the DEFPROT attribute specified and/or the resources and/or generic equivalent identified below are

owned.

____ The TSS 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-7328r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZJES0031
Rule Title: JES2 output devices are improperly protected.

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.

Check Content:

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

- TSSCMD5.RPT(WHOOWTR)

Refer to the following reports produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

- EXAM.RPT(SUBSYS)

b) Review the following resources in the WRITER resource class:

JES2.(backstop entry)

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.

c) Ensure the following items are in effect:

1) The JES2. resource is owned in the WRITER resource class.

2) The ownership of all WRITER resources is appropriate.

d) If all of the items in (c) are true, there is NO FINDING.

e) If any item in (c) is untrue, this is a FINDING.

Fix Text: Ensure the following items are in effect:

1) The JES2. resource is owned in the WRITER resource class.

For Example:

The following command may be used to establish default protection for resources defined to the WRITER resource class:

TSS ADDTO(deptacid) WRITER(JES2.)

2) The ownership of all WRITER resources is appropriate.

Grant read access to authorized users for each of the following WRITER resource class output destinations:

JES2.LOCAL.devicename
JES2.LOCAL.OFF*.JT
JES2.LOCAL.OFF*.ST
JES2.LOCAL.PRT*
JES2.LOCAL.PUN*
JES2.NJE.nodename
JES2.RJE.devicename

The following is an example of granting operators with a profile ACID of jesopracid permission to off load SYSOUT data sets into any SPOOL off load processor after obtaining permission from the IAO:

TSS PERMIT(jesopracid) WRITER(JES2.LOCAL.OFF*.ST) -
ACCESS(READ) ACTION(AUDIT)

The resource definition should be generic if all of the resources of the same type have identical access controls (e.g., if all off load transmitters are equivalent).

CCI: CCI-000213

Group ID (Vulid): V-6922
Group Title: ZJES0032
Rule ID: SV-74873r1_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..

Check Content:

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

- Classification of System

- SENSITIVE.RPT(WHOHWTR)

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 TSS WRITER resource class in the RDT has the DEFPROT attribute specified and/or the resources and/or generic equivalent identified below are owned.

____ The TSS 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-7333r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZJES0041

Rule Title: JESSPOOL resources are improperly protected.

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.

Check Content:

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

- TSSCMD5.RPT(WHOOJESS)

Refer to the following report produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

Automated Analysis

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

- PDI(ZJES0041)

b) Ensure that the resource localnodeid. is owned in the JESSPOOL class.

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.

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

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

Fix Text: Ensure that the resource localnodeid. is owned in the JESSPOOL class.

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

(1) The following command may be used to establish default protection for resources defined to the JESSPOOL resource class:

```
TSS ADDTO(deptacid) JESSPOOL(localnodeid.)
```

Due to the protection established with the previous command, the following command should be issued to ensure users are able to access their own spool data:

```
TSS PERMIT(ALL) JESSPOOL(localnodeid.%) ACCESS(ALL)
```

CCI: CCI-000213

Group ID (Vulid): V-6924
Group Title: ZJES0042
Rule ID: SV-7330r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZJES0042
Rule Title: JESNEWS resources are improperly protected.

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.

Check Content:

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

- SENSITVE.RPT(WHOHOPER)

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) Ensure that 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.

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.

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

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

Fix Text: Ensure that 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.

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.

For Example:

The following command example may be used to allow all valid TOP SECRET users read access to the JES News data set:

```
TSS PERMIT(ALL) JESSPOOL(localnodeid.jesid.$JESNEWS.*.*JESNEWS) –  
ACCESS(READ)
```

The following is a sample command to allow production control personnel with a profile ACID of prodacid to update the JES News data set:

```
TSS PERMIT(prodacid) OPERCMDS(JES2.UPDATE.JESNEWS) –  
ACCESS(CONTROL) ACTION(AUDIT)
```

CCI: CCI-000213

CCI: CCI-001762

CCI: CCI-002234

Group ID (Vulid): V-6925

Group Title: ZJES0044

Rule ID: SV-7335r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZJES0044

Rule Title: JESTRACE and/or SYSLOG resources are improperly protected.

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.

Check Content:

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

- SENSITIVE.RPT(WHOHJESS)

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

- TSSCMDS.RPT(WHOHJESS)

Refer to the following report produced by the z/OS Data Collection:

- PARMLIB(JES2 parameters)

Review the following resources defined to the JESSPOOL resource class:

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.*.*.*.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) ACID(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:

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:

ACID(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.

For Example:

TSS ADD(dept-acid) JESSPOOL(localnodeid)

TSS PERMIT(<syspau>) JESSPOOL(localnodeid.JES2.\$TRCLOG.) ACCESS(ALL)

TSS PERMIT(<secaudt>) JESSPOOL(localnodeid.JES2.\$TRCLOG.) ACCESS(ALL)

TSS PERMIT(<syspau>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(ALL)

TSS PERMIT(<secaudt>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(ALL)

TSS PERMIT(<appdaudt>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(READ)

TSS PERMIT(<appsaudt>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(READ)

or

TSS PERMIT(<syspau>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(ALL)

TSS PERMIT(<secaudt>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(ALL)

TSS PERMIT(<appdaudt>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(READ)

TSS PERMIT(<appsaudt>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-001762

Group ID (Vulid): V-6926

Group Title: ZJES0046

Rule ID: SV-7337r3_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.

Check Content:

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

- SENSITIVE.RPT(WHOHJESS)
- TSSCMD5.RPT(#ALL)

Verify that the accesses to the JESSPOOL resources are properly restricted. If the following guidance is true, this is not a finding.

Review the JESSPOOL report for resource permissions with the following naming convention. These permissions 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 user ACID associated with the job. This is the user ACID TSS 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 shall have access to their own JESSPOOL resources. Permission can be granted by resource permission JESSPOOL(localnodeid.%) ACCESS(ALL). This permission can be given to profiles, individual user, and/or the ALL record. Access to this resource does not require logging.

Ensure the following items are in effect:

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel, with access of ALL. 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. 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 (?).

All users shall have access to their own JESSPOOL resources. Permission can be granted by resource permission JESSPOOL(localnodeid.%) ACCESS(ALL). This permission can be given to profiles, individual user, and/or the ALL record. Access to this resource does not require logging.

Example:
TSS ADDTO(deptacid) JESSPOOL(localnode.)

TSS PERMIT(ALL) JESSPOOL(localnode.%.) ACCESS(ALL)

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel, with access of ALL. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc)

Example:

TSS PERMIT(syspautd) JESSPOOL(localnodeid.) ACCESS(ALL) ACTION(AUDIT)

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. 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.

Example:

TSS PERMIT(Project1-profile) JESSPOOL(localnodeid.UMO) ACCESS(ALL)

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

Rule ID: SV-7339r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZJES0051

Rule Title: JES2.** resource is improperly protected.

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.

Check Content:

JES2 Command Resource Definition

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

- TSSCMDS.RPT(WHOOOPER)

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) If the JES2. resource is owned in 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.

c) If the JES2. resource is NOT owned, or is owned inappropriately, in the OPERCMDS class, this is a FINDING.

Fix Text: The JES2. resource must be owned in the OPERCMDS class.

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.

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. To control access to JES2 system commands, the following recommendations will be applied when implementing security:

For Example:

The following command may be used to establish default protection for JES2 system commands defined to the OPERCMDS resource class:

TSS ADDTO(deptacid) OPERCMDS(JES2.)

CCI: CCI-000213

Group ID (Vulid): V-6928

Group Title: ZJES0052

Rule ID: SV-17409r2_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.

Check Content:

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

- SENSITIVE.RPT(WHOHOPER)

Automated Analysis

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

- PDI(ZJES0052)

b) 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.

c) 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.

d) If either (b) or (c) 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. To control access to JES2 system commands, the following recommendations will be applied when implementing security:

Ensure access to JES2 system commands defined in the "Controls on JES2 System Commands" table, in the z/OS STIG Addendum restricts access to the appropriate personnel (e.g., operations staff, systems programming personnel, general users) and logged if indicated.

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

The following is a sample command to allow operators with a profile ACID of opracid to use the \$DS command:

```
TSS PERMIT(opracid) OPRCMDS(JES2.DISPLAY.STC) ACCESS(READ)
```

The following is a sample command to allow operators with a profile ACID of opracid to use the \$DM command:

```
TSS PERMIT(opracid) OPERCMDS(JES2.SEND.MESSAGE) -  
ACCESS(READ) ACTION(AUDIT)
```

The following is a sample command to allow operators with a profile ACID of opracid to use the \$B command:

```
TSS PERMIT(opracid) OPERCMDS(JES2.BACKSP.DEV) -  
ACCESS(UPDATE) ACTION(AUDIT)
```

The following is a sample command to allow operators with a profile ACID of opracid to use the \$ZI command:

```
TSS PERMIT(opracid) OPERCMDS(JES2.HALT.INITIATOR) -  
ACCESS(CONTROL) ACTION(AUDIT)
```

The following is a sample command to allow operators with a profile ACID of opracid to use the \$ZSPOOL command:

```
TSS PERMIT(opracid) OPERCMDS(JES2.HALT.SPOOL) -  
ACCESS(CONTROL) ACTION(AUDIT)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-54

Group Title: ZJES0060

Rule ID: SV-7347r5_rule

Severity: CAT II

Rule Version (STIG-ID): ZJES0060

Rule Title: Surrogate users or Cross-Authorized ACIDs must be controlled in accordance with the proper requirements.

Vulnerability Discussion: Surrogate users/Cross-Authorized ACIDs 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/Cross-Authorized ACIDs run with the identity of the execution user. Failure to properly control surrogate users/Cross-Authorized ACIDs 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.

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)

If no XA ACID entries exist in the above reports, this is not applicable.

For each ACID identified in the XA ACID entries, if the following items are true regarding ACID permissions this is not a finding.

___ ACID permission (XA ACID) is logged (ACTION = AUDIT), only for Privileged USERIDS (MASTER, SCA, DCA, VCA, ZCA) if they are XAUTH; at the discretion of the

ISSM/ISSO scheduling tasks may be exempted from logging.

___ 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 each ACID identified in the XA ACID entries, ensure the following items are in effect regarding ACID permissions:

ACID permission (XA ACID) is logged (ACTION = AUDIT), at the discretion of the ISSM/ISSO scheduling tasks may be exempted from logging.

ACID permission (XA ACID) is logged (ACTION = AUDIT), for Privileged users (MSCA, SCA, DCA, VCA, ZCA).

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 Cross-Authorized ACIDs:

Keep ACID cross authorization of ACIDs outside of those granted to the scheduling software to a minimum number of individuals.

The simplest configuration is to have no ACID Cross Authorization except for the appropriate Scheduling task/software for production scheduling purposes as documented.

Temporary Cross Authorization of the production batch ACID 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, ACID Cross Authorization usage shall not become the default for all jobs submitted by individual users (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..

Grant access to the user ACID for each cross-authorized ACID required:

For Example:

TSS PERMIT(ACID) ACID(Cross-Authorized ACID) ACTION(AUDIT)

For production ACIDs being used by CONTROLM:

TSS PER(CONTROLM)ACID(production user ACID)

CCI: CCI-000213

CCI: CCI-002233

CCI: CCI-002234

Group ID (Vulid): V-31

Group Title: ZSMS0010

Rule ID: SV-7356r5_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.

Check Content:

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

- SENSITVE.RPT(ZSMS0010)

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 TSS resources are owned or DEFPROT is specified for the resource class.

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 NONE.

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 of NONE.

If the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE and STGADMIN.IGG.CATALOG.SECURITY.BOTH are both defined, STGADMIN.IGG.CATALOG.SECURITY.BOTH takes precedence.

___ 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.

___ 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 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 resources and/or generic equivalent are followed.

The TSS resources are owned and/or DEFPROT is specified for the resource class.

Configure resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE with no access.

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 = NONE.

Configure STGADMIN.IGG.CATALOG.SECURITY.BOTH to have READ access for all.

TSS ADD(ADMIN) IBMFAC(STGADMIN)

or

TSS REPLACE(RDT) RESCLASS(IBMFA) ATTR(DEFPROT)

The STGADMIN.DPDSRN.olddsrn is restricted to System Programmers and all access is logged.

Example:

TSS PERMIT(syspau) IBMFAC(STGADMIN.DPDSRN.olddsrn) -
ACCESS(READ) ACTION(AUDIT)

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to System Programmers and all access is logged.

Example:

TSS PERMIT(syspau) IBMFAC(STGADMIN.IGD.ACTIVATE.CONFIGURATION) -
ACCESS(READ) ACTION(AUDIT)

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to System Programmers and Security personnel and all access is logged.

Example:

TSS PERMIT(secpau) IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS) -
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(secdaud) IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS) -
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(syspau) IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS) -
ACCESS(READ) ACTION(AUDIT)

The following resources and prefixes may be available to the end-user.

STGADMIN.ADR.COPY.CNCURNT

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:

TSS PERMIT(endusers) IBMFAC(STGADMIN.ADR.COPY.CNCURRNT.) -
ACCESS(READ)

The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and System programmers.

STGADMIN.IDC.DCOLLECT

Example:

TSS PERMIT(appsaudt) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(autoaudt) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(dasbaudt) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(dasdaudt) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(syspaudt) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)

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:

TSS PERMIT(appsaudt) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)
TSS PERMIT(dasbaudt) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)
TSS PERMIT(dasdaudt) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)
TSS PERMIT(syspaudt) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)

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:

TSS PERMIT(dasbaudt) IBMFAC(STGADMIN.ADR) ACCESS(READ)
TSS PERMIT(dasdaudt) IBMFAC(STGADMIN.ADR) ACCESS(READ)
TSS PERMIT(syspauadt) IBMFAC(STGADMIN.ADR) ACCESS(READ)

The following Storage Administrator functions prefix is restricted to DASD managers and System programmers and all access is logged.

STGADMIN.ADR.STGADMIN.

Example:

TSS PERMIT(dasbaudt) IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ) –
ACTION(AUDIT)
TSS PERMIT(dasdaudt) IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ) –
ACTION(AUDIT)
TSS PERMIT(syspauadt) IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ) –
ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6933
Group Title: ZSMS0012
Rule ID: SV-7351r4_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.

Check Content:

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

- SENSITVE.RPT(ZSMS0012)

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 TSS resources are owned or DEFPROT is specified for the resource class.

___ The TSS 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 zOS 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 TSS resources as designated in the above table are owned and/or DEFPROT is specified for the resource class.

The TSS 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:

```
TSS ADD(dept-acid) PROGRAM(ACBFUTO2)
TSS PERMIT(audtaudt) PROGRAM(ACBFUTO2)
TSS PERMIT(dasdaudt) PROGRAM(ACBFUTO2)
TSS PERMIT(secaudt) PROGRAM(ACBFUTO2)
TSS PERMIT(syspauudt) PROGRAM(ACBFUTO2)
TSS PERMIT(tstcaudt) PROGRAM(ACBFUTO2)
```

CCI: CCI-000213

Group ID (Vulid): V-3895

Group Title: ZSMS0020

Rule ID: SV-7358r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZSMS0020

Rule Title: DFSMS control data sets must be 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.

Check Content:

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

- SENSITVE.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

If the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALL access to only systems programming personnel, this is not a finding.

If the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict UPDATE and ALL 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: 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

Assign ownership of the data sets, replacing user-id with a user, department, or division that administer access to the SMS control data sets, and data name with the prefix of the SMS control data sets:

TSS ADD(user-id) DSN(data name)

Ensure the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALL access to only z/OS systems programming personnel.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control datasets.

Permit access to those personnel who manage the SMS environment, replacing user-id with the userid of the user or a Group profile:

TSS PERMIT(user-id) DSN(data name) ACC(UPDATE) ACTION(AUDIT)

Permit access to those personnel that perform maintenance on these data sets:

TSS PERMIT(user-id) DSN(data name) ACC(ALL) ACTION(AUDIT)

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.

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)

Automated Analysis

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

- PDI(ZSMS0022)

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 COMMD5 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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Review the SYS1.PARMLIB(IEFSSNxx) data set for 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.

IACControls: 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-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.

Check Content:

Locate the SSH daemon configuration file.

May be found in /etc/ssh/ directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is not active there is no finding.

Examine SSH daemon configuration file. If the variables 'Protocol 2,1' or 'Protocol 1' are defined on a line without a leading comment, 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.

Check Content:

Locate the SSH daemon configuration file.

May be found in /etc/ssh/ directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is not active there is no finding.

Examine SSH daemon configuration file.

sshd_config

If there are no Ciphers lines or the ciphers list contains any cipher not starting with "3des" or "aes", this is a finding.

If the MACs line is not configured to "hmac-sha1" or greater this is a finding.

Examine the z/OS-specific sshd server system-wide configuration

zos_sshd_config

If any of the following is untrue this is a finding.

FIPSMODE=YES

CiphersSource=ICSF

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.

Check Content:
Locate the SSH daemon configuration file.
May be found in /etc/ssh/ directory.
Alternately:
From UNIX System Services ISPF Shell navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SSH Daemon is not active there is no finding.

Examine SSH daemon configuration file.
If Banner statement is missing or configured to none this is a finding.

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.

Check Content:

Locate the SSH daemon configuration file.

May be found in /etc/ssh/ directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is not active there is no finding.

Examine SSH daemon configuration file.

If ServerSMF is not coded with ServerSMF TYPE119_U83 or 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.

Check Content:

Locate the SSH daemon configuration file.

May be found in /etc/ssh/ directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is not active there is no finding.

Examine the 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

Locate the z/OS-specific sshd server system-wide configuration file.

zos_sshd_config

May be found in /etc/ssh/ directory.

Ensure that a HostKeyRingLabel line is coded and not commented out.

If either of the above is not 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.

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

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(TSOUADS)

Please provide a list of all emergency userids available to the site along with the associated function of each.

b) If SYS1.UADS userids are limited and reserved for emergency purposes only, there is NO FINDING.

c) 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-297r4_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, MOUNT, TESTAUTH, 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

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

- SENSITVE.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.

IACControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- EXAM.RPT(PARMLIB) - Refer to the IEASYSxx listing(s).

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI (ZUSS0011)

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.

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-7246r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZUSS0012

Rule Title: z/OS UNIX BPXPRMxx security parameters in PARMLIB must be 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

Check Content:

a) 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 /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID
SETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS

Automated Analysis requires Additional Analysis.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZUSS0012)

b) If the required parameter keywords and values are defined, there is NO FINDING.

c) If the required parameter keywords and values are not defined, this is a FINDING.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- PDI(ZUSS0012)

b) If the required parameter keywords and values are defined, there is NO FINDING.

c) 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.

IACControls: DCCS-1, DCCS-2

Check Content:

a) Review the logical parmlib 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.

b) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(EAUTOM)

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 any deviation from the required values, 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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following reports produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(EINETD)
- USSCMDS.RPT(ESERV)

b) If all the services in the Restricted Network Services Table in the z/OS STIG Addendum are not found in or are commented out of the /etc/inetd.conf file, there is NO FINDING.

c) If any Restricted Network Services are 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.

IACControls: 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.

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-7405r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZUSS0021

Rule Title: BPX resource(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.

Check Content:

a) Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- TSSCMDS.RPT(WHOOIBMF)
- SENSITIVE.RPT(WHOHIBMF)

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 IBMFAC resource class:

- 1) The TSS owner defined for the BPX resource.
- 2) There are no TSS rules that allow access to the BPX resource.
- 3) There are no TSS rules for BPX.SAFFASTPATH defined.
- 4) The TSS 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: Because they convey especially powerful privileges, the settings for BPX.DAEMON, BPX.SAFFASTPATH, BPX.SERVER, and BPX.SUPERUSER require special attention.

Review the following items for the IBMFAC resource class:

- 1) The TSS owner defined for the BPX resource.
- 2) There are no TSS rules that allow access to the BPX resource.
- 3) There is no TSS rules for BPX.SAFFASTPATH defined.
- 4) The TSS rules for each of the BPX resources listed in General Facility Class BPX Resources Table, in the zOS STIG Addendum restrict access to appropriate system tasks or systems programming personnel. Access can be permitted only to users with a requirement for the resource that is documented to the IAO. Access to BPX.DAEMON must be restricted to the z/OS UNIX kernel userid, z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons (e.g., web servers). when BPX.SAFFASTPATH is defined, calls to the ACP are not performed for file accesses and there is no audit trail of access failures. This configuration is unacceptable. Therefore BPX.SAFFASTPATH must not be used on any system.

For Example:

The following commands can be used to provide the required protection:

TSS ADD(ADMIN) IBMFAC(BPX.)

TSS PERMIT(ALL) IBMFAC(BPX.SAFFASTPATH) ACCESS(NONE)

NOTE:

The PERMIT command for BPX.SAFFASTPATH must be executed on TOP SECRET systems. If access to BPX.SAFFSTPATH were allowed, z/OS UNIX would perform permission bit checking internally instead of calling the ACP. On TOP SECRET systems this would bypass any audit trail of violations. In addition, the z/OS UNIX kernel userid (OMVS is the example in this section) must not have the TOP SECRET NORESCHK privilege. Having that privilege would allow access to BPX.SAFFASTPATH even though the access restriction was in place.

CCI: CCI-000213

CCI: CCI-001764

Group ID (Vulid): V-6970

Group Title: ZUSS0022

Rule ID: SV-19747r4_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.

Check Content:

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

- TSSCMD5.RPT(WHOOSURR)
- SENSITVE.RPT(WHOHSURR)

Automated Analysis

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

- PDI(ZUSS0022)

Ensure that the following resources and/or generic equivalents are properly protected according to the requirements specified below for the SURROGAT resource class. If the following guidance is true, this is not a finding.

____ The TSS resources and/or generic equivalent for BPX. is owned or DEFPROT is specified for the resource class.

____ The TSS resource access authorizations restrict BPX.SRV.user to system software processes (e.g., web servers) that act as servers under z/OS UNIX.

Fix Text: The Systems Programmer and IAO will ensure that BPX. SRV.userid resources are properly protected and access is restricted to appropriate system tasks or systems programming personnel.

SURROGAT class BPX resources are used in conjunction with server applications that are performing tasks on behalf of client users that may not supply an authenticator to the server. This can be the case when clients are otherwise validated or when the requested service is performed from userids representing groups.

a) Ensure there is a TSS owner defined for the (BPX.) SURROGAT class resource.

For Example:

TSS ADD(dept) SURROGAT(BPX.)

b) Ensure the TSS rules for all BPX.SRV.user SURROGAT resources restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX.

For Example:

TSS PERMIT(<websrv>) SURROGAT(BPX.SRV.<webadm>)

ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-6972

Group Title: ZUSS0023

Rule ID: SV-19749r3_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.

Check Content:

a) Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- TSSCMDS.RPT(WHOOUNI)
- SENSITVE.RPT(WHOHUNI)

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:

- 1) The TSS owner defined for the SUPERUSER resource.
- 2) There are no TSS rules that allow access to the SUPERUSER resource.
- 3) There is no TSS rule for CHOWN.UNRESTRICTED defined.
- 4) The TSS 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.

Review the following items for the UNIXPRIV resource class:

- 1) The TSS owner defined for the SUPERUSER resource.
- 2) There are no TSS rules that allow access to the SUPERUSER resource.

- 3) There is no TSS rule for CHOWN.UNRESTRICTED defined.
- 4) The TSS 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.

Sample Commands:

```
TSS ADD(dept) UNIXPRIV(SUPERUSE)
TSS PERMIT(<SYSPAUDT>) UNIXPRIV(SUPERUSER.FILESYS.) ACCESS(READ)
/* where SUPERUSER.FILESYS. represents one of the resources listed in the
UNIXPRIV CLASS RESOURCES table in the Addendum */
```

To determine the current active setting of CHOWNURS, issue a TSS MODIFY STATUS(BASE) command.

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.

IACControls: 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.

IACControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

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

- SENSITVE.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.

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.

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.

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

Check Content:

Refer to the following reports produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(SFPERM)
- USSCMDS.RPT(EAUTOM)

Refer to the following report produced by the IBM Communications Server Data Collection:

- PDI(ZUSS0035)

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 FILE SECURITY SETTINGS Table in the z/OS STIG Addendum. If the guidance is true, this is not a finding.

NOTE:

Some of the files listed in the SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum are not used in every configuration. Absence of any of the files is not considered a finding.

NOTE: The names of the MapName files are site-defined. Refer to the listing in the EAUTOM report.

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.

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

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(OWDIR)

b) 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".

c) 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".

d) 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".

e) If (b), (c), or (d) 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.

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.

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.

IAControls: DCCS-1, DCCS-2

Check Content:

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

ACF2

- ACF2CMDS.RPT(OMVSUSER)
- ACF2CMDS.RPT(LOGONIDS)

RACF

- RACFCMDS.RPT(LISTUSER)

TSS

- TSSCMDS.RPT(@ACIDS)

b) If OMVS is defined as follows, there is NO FINDING:

- 1) No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- 2) Default group specified as OMVSGRP or STCOMVS
- 3) UID(0)
- 4) HOME directory specified as "/"
- 5) Shell program specified as "/bin/sh"

c) If OMVS is not defined as specified in (b) above, this is a FINDING

Fix Text: The systems programmer will verify that OMVS is defined as specified below:

- 1) No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- 2) Default group specified as OMVSGRP or STCOMVS
- 3) UID(0)
- 4) HOME directory specified as "/"
- 5) Shell program specified as "/bin/sh"

CCI: CCI-000764

Group ID (Vulid): V-6988

Group Title: ZUSS0044

Rule ID: SV-87471r1_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.

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:

TSS LIST(superuser userid) DATA(ALL)

Alternately refer to TSS Data Collection:

- TSSCMD5.RPT(@ACIDS)

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
- 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-87477r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZUSS0045

Rule Title: The user account for the z/OS UNIX (RMFGAT) 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.

Check Content:

RMFGAT is the userid for the Resource Measurement Facility (RMF) Monitor III Gatherer. If RMFGAT is not defined this is not applicable.

From a command input screen enter:

TSS LIST (RMFGAT) DATA ALL

Alternately:

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

- TSSCMD5.RPT(@ACIDS)

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 RMFGAT user account is defined 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-7294r3_rule

Severity: CAT I

Rule Version (STIG-ID): ZUSS0046

Rule Title: UID(0) must be properly 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.

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.

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-7941r5_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: Top Secret ACIDs that use z/OS UNIX facilities must be properly defined. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Check Content:

If this is a classified system, this is not applicable.

From a command line issue the following command:

Note: One must have appropriate access to perform this command (have the site security officer issue the command)

TSS MODIFY STATUS

Examine the following option:
UNIQUEUSER

Alternately:

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

- TSSCMDS.RPT(STATUS)
- TSSCMDS.RPT(OMVSUSER)

Note: This check applies to any user identifier (ACID) used to model OMVS access on the mainframe. This includes OMVSUSR; MODLUSER, and BPX.UNIQUE.USER.

If MODLUSER is specified then UNIQUEUSER must be specified as "ON".

If user identifier (ACID) used to model OMVS user account is defined as follows, this is not 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.

Define the user identifier (ACID) used to model OMVS user account with a non-writable home directory, such as "\" root, and a non-executable, but existing, binary file, "/bin/false" or "/bin/echo."

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.

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-7000
Group Title: ZUSST050
Rule ID: SV-7303r4_rule
Severity: CAT II
Rule Version (STIG-ID): ZUSST050
Rule Title: The z/OS Default profiles must not be defined in TSS OMVS UNIX security parameters for classified systems.

Vulnerability Discussion: TSS UNIQUUSER control option will automatically assign a UID to any user who logs on to OMVS without an OMVS segment. Parameter settings in the TSS impact the security level of z/OS UNIX. In classified systems user access will not be determined by default.

Check Content:
If the system is not classified this is not applicable.

From a command line issue the following command:
Note: One must have appropriate access to perform this command (have the site security officer to issue command).

TSS MODIFY STATUS

Examine the following options:
UNIQUUSER

Alternately:
Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(STATUS)
- System Classification

Automated Analysis requires Additional Analysis.
Refer to the following report produced by the TSS Data Collection:

- PDI(ZUSST050)

If system is classified and UNIQUUSER is off i.e., (UNIQUUSER(OFF)) there is no finding.

Fix Text: Ensure that Use of the OMVS default UIDs will not be allowed on any classified system.

Set Control Option UNIQUUSER off.

CCI: CCI-000366

Group ID (Vulid): V-6948

Group Title: ZUSST052

Rule ID: SV-7249r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZUSST052

Rule Title: TSS UNIX control option CHOWNURS must be properly set.

Vulnerability Discussion: Parameter settings in TSS impact the security level of z/OS UNIX.

IAControls: DCCS-1, DCCS-2

Check Content:

For CA-Top Secret Release 15 and above this is Not Applicable.

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

- TSSCMDS.RPT(STATUS)

Automated Analysis

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

- PDI(ZUSST052)

If the CHOWNURS control option is set to CHOWNURS(OFF), this is not a finding.

Fix Text: The IAO must set the CHOWNURS control option to CHOWNURS(OFF).

TSS MODIFY CHOWNURS(OFF)

CCI: CCI-000366

Group ID (Vulid): V-7021

Group Title: ZUSST060

Rule ID: SV-7383r2_rule

Severity: CAT I

Rule Version (STIG-ID): ZUSST060

Rule Title: The HFSSEC resource class is not defined with DEFPROT.

Vulnerability Discussion: The HFSSEC resource class configuration settings in the ACP impact the security level of z/OS UNIX.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMDS.RPT(STATUS)
- TSSCMDS.RPT(#RDT)

Automated Analysis

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

- PDI(ZUSST060)
- b) If the Control Option is HFSSEC(OFF), this is NOT APPLICABLE.
- c) If the DEFPROT attribute is specified for the HFSSEC resource class in the RDT, there is NO FINDING.
- d) If (c) above is untrue, this is a FINDING.

Fix Text: Ensure that the HFSSEC resource class has the attribute DEFPROT.

For Example:

TSS REPLACE(RDT) RESCLASS(HFSSEC) ATTR(DEFPROT)

CCI: CCI-000213

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.

IAControls: DCCS-1, DCCS-2, IAAC-1

Check Content:

a) Have the IAO and VTAM Systems Programmer supply the following information:

- Documentation regarding terminal naming standards.
- Documentation of all procedures controlling terminal logons to the system.
- A complete list of all USS commands used by terminal users to log on to the system.
- Members and data set names containing USSTAB and LOGAPPL definitions of all terminals that can log on to the system (e.g., SYS1.VTAMLST).
- 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.

c) If USSTAB definitions are used for any unsecured terminals (e.g., dial up terminals or terminals attached to the Internet such as TN3270 or KNET 3270 emulation), this is a 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-7360r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZVTM0018

Rule Title: The System datasets used to support the VTAM network are improperly 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.

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:

- SENSITVE.RPT(VTAMRPT)

Automated Analysis

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

- PDI(ZVTM0018)

b) Ensure that TSS 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: Ensure that TSS 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.

The following sample TSS commands show proper permissions for VTAM datasets (replace "profile" with the profile name of the network systems programming staff authorities) :

```
TSS PERMIT(profile) DSN(SYS1.VTAM.) ACC(ALL)
TSS PERMIT(profile) DSN('SYS1.VTAMLIB.) ACC(ALL)
TSS PERMIT(profile) DSN(SYS1.VTAM.SISTCLIB.) ACC(ALL)
TSS PERMIT(profile) DSN(SYS3.VTAM.) ACC(ALL)
TSS PERMIT(profile) DSN(SYS3.VTAMLIB.) ACC(ALL)
```

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.

IACControls: 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.

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 webadmg1, 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 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 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-7266r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZWAS0030
Rule Title: The CBIND Resource(s) for the WebSphere Application Server is(are) not protected 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.

Check Content:

a) Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- TSSCMDS.RPT(WHOOCBIN)
- TSSCMDS.RPT(WHOHCBIN)
- SENSITIVE.RPT(WHOHCBIN)

b) Ensure the following items are in effect for CBIND resource protection:

- 1) The CB. resource is owned appropriately in the BIND resource class.
- 2) Access to the CB.BIND.server_name and CB.server_name resources is restricted to WAS server (STC) ACIDs and systems management ACIDs (e.g., WebSphere administrator ID).

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 the following items are in effect for CBIND resource protection:

- 1) The CB. resource is owned appropriately in the BIND resource class.

For Example:

TSS ADD(cbowner) CBIND(CB)

- 2) Access to the CB.BIND.server_name and CB.server_name resources is restricted to WAS server (STC) ACIDs and systems management ACIDs (e.g., WebSphere administrator ID).

For Example:

The WebSphere administrator ID needs read authority to the CB.BBOASR1 and CB.BIND.BBOASR1 servers:

TSS PERMIT(was_admin_acid) CBIND(CB.BBOASR1) ACCESS(READ)

TSS PERMIT(was_admin_acid) CBIND(CB.BIND.BBOASR1) ACCESS(READ)

NOTE: When adding a new server, all systems management userids (e.g., WebSphere administrator ID) must be authorized to have read access to the CB.server_name and CB.BIND.server_name resources.

CCI: CCI-000213

Group ID (Vulid): V-3900

Group Title: ZWAS0040

Rule ID: SV-3900r3_rule

Severity: CAT I

Rule Version (STIG-ID): ZWAS0040

Rule Title: Vendor-supplied user accounts for the WebSphere Application Server must be 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.

Severity Override Guidance:

IAO will ensure that CBADMIN user password is changed from default.

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.

IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(AHTTPD)

Collect the following information for each IBM HTTP server:

- The JCL procedure library and member name used to start each IBM HTTP server. DOC(IHSPROCS)
- For each IBM HTTP server, supply the following information:

Web server ID defined to the ACP

Web server administration group defined to the ACP

Web server standard HFS directory

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-7259r5_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

Check Content:

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).

Collect the following Information for Websphere MQ and MQSeries 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.

Automated Analysis requires Additional Analysis.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZWMQ0011)

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, this is not a finding.

If the following guidelines are true for each channel definition displayed from the DISPLAY CHANNEL command, this is not a finding.

___ Verify that each WebSphere MQ channel is using SSL by checking for the SSLCIPH parameter, which must specify a FIPS 140-2 compliant value of the following: (Note: Both ends of the channel must specify the same 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

___ Repeat the above step for each queue manager ssid identified.

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 (Vulid): 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.

IAControls: DCCS-1, DCCS-2

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). 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 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:

- MQSRPT(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:

- MQSRPT(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:

- MQSRPT(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:

- MQSRPT(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.

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.

IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

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).

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZWMQ0020)

b) Review the ssid report(s) and perform the following steps:

- 1) Find the DISPLAY SECURITY command to locate the start of the security parameter settings.
- 2) Review the CSQH015I and CSQH016I messages to determine the Timeout and Interval parameter settings respectively.
- 3) Repeat these steps for each queue manager ssid.

The standard values are:

TIMEOUT(15)

INTERVAL(5)

c) If the Timeout and Interval values conform to the standard values, there is NO FINDING.

d) If the Timeout and/or Interval values do not conform to the standard values, this is a FINDING.

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-7527r1_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.

Check Content:

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

- TSSCMDS.RPT(#STC)
- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(FACLIST) - Preferred report containing all control option values in effect including default values.
- TSSCMDS.RPT(TSSPRMFL) - Alternate report containing only control option values explicitly coded at TSS startup.

NOTE: The FACLIST report must be created by security personnel. The TSSPRMFL report can be used if security personnel have not executed the required steps documented in the TSS Data Collection.

Provide a list of all WebSphere MQ Subsystem Ids (Queue managers) and Release levels.

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 ACID.
- 2) Each ssidMSTR and ssidCHIN started task is defined to the STC record with a unique ACID.
- 3) Each ssidMSTR started task ACID has a corresponding WebSphere MQ MASTFAC defined.
- 4) WebSphere MQ queue manager facilities is defined to the Facility Matrix Table using the following sample commands:

```
FAC(USERxx=NAME=ssidMSTR,MODE=FAIL,PGM=CSQ,ID=xx,ACTIVE)
FAC(ssidMSTR=SHRPRF,ASUBM,NOABEND,MULTUSER,XDEF,LUMSG)
FAC(ssidMSTR=STMSG,SIGN(S),INSTDATA,NORNDPW,AUTHINIT)
FAC(ssidMSTR=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC)
FAC(ssidMSTR=LCFTRANS,IJU,MSGLC,NOTRACE,NOEODINIT)
FAC(ssidMSTR=NODORMPW,NONPWR)
FAC(ssidMSTR=LOG(INIT,SMF,MSG,SEC9))
FAC(ssidMSTR=DOWN=GLOBAL,LOCKTIME=00,DEFACID=(*NONE*))
```

Fix Text: 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 WebSphere MQ started task is associated with a unique ACID.
- 2) Each WebSphere MQ started task is defined to the STC record with a unique ACID.
- 3) Each ssidMSTR STC ACID has a corresponding WebSphere MQ MASTFAC as defined in the z/OS.

i.e. A Started Task Table entry exists for each queue manager started task procedure xxxxMSTR and distributed queuing started task procedure xxxxCHIN. A corresponding userid for each started task exists. Queue manager and channel initiator started tasks will not be defined with the BYPASS attribute.

- 4) WebSphere MQ queue manager facilities are defined using the control options as specified below:

Define each queue manager xxxxMSTR to the TOP SECRET Facility Matrix Table using the following sample commands:

```
FACILITY(USERxx=NAME=xxxxMSTR)
FACILITY(xxxxMSTR=MODE=FAIL,PGM=CSQ,ID=xx)
FACILITY(xxxxMSTR=ACTIVE,SHRPRF,ASUBM,NOABEND)
FACILITY(xxxxMSTR=MULTUSER,XDEF,LUMSG,STMSG,SIGN(S))
FACILITY(xxxxMSTR=INSTDATA,NORNDPW,AUTHINIT)
FACILITY(xxxxMSTR=NOPROMPT,NOAUDIT,RES,WARNPW)
FACILITY(xxxxMSTR=NOTSOC,LCFTRANS,IJU,MSGLC,NOTRACE)
FACILITY(xxxxMSTR=NOEODINIT,NODORMPW,NONPWR)
(INIT,SMF,MSG,SEC9))
FACILITY(xxxxMSTR=DOWN=GLOBAL,LOCKTIME=00,DEFACID=(*NONE*))
```

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.

IACControls: 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 JESMSG LG 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 JESMSG LG file of the ssidMSTR active task(s). Find the CSQY122I message to obtain the ARCPFRX1 and ARCPFRX2 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-7535r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0049

Rule Title: WebSphere MQ security class(es) is(are) defined improperly.

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.

Check Content:

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

- TSSCMDS.RPT(#RDT)
- TSSCMDS.RPT(WHOOMADM)
- TSSCMDS.RPT(WHOOMCMD)
- TSSCMDS.RPT(WHOOMCON)
- TSSCMDS.RPT(WHOOMNLI)
- TSSCMDS.RPT(WHOOMPRO)
- TSSCMDS.RPT(WHOOMQUE)
- TSSCMDS.RPT(WHOOXADM)
- TSSCMDS.RPT(WHOOXNLI)
- TSSCMDS.RPT(WHOOXPRO)
- TSSCMDS.RPT(WHOOXQUE)
- TSSCMDS.RPT(WHOOXTOP)

Ensure the following WebSphere MQ resource classes are defined to the TSS RDT:

MQADMIN

MQCONN

MQCMDS
MQNLIST
MQPROC
MQQUEUE

For V7.0.0 and above:

MXADMIN
MXNLIST
MXPROC
MXQUEUE
MXTOPIC

Ensure that each ssid. resource is defined in each of the above resource classes.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

NOTE: If both MQADMIN and MXADMIN resource classes are not defined to the RDT record, no security checking is performed.

Fix Text: The IAO will ensure that all WebSphere MQ resources are defined to TSS.

The following should be defined to the RDT:

MQADMIN
MQCONN
MQCMDS
MQNLIST
MQPROC
MQQUEUE

For V7.0.0 and above:

MXADMIN
MXNLIST
MXPROC
MXQUEUE
MXTOPIC

Use the following commands to define (establish ownership of) resources for each WebSphere MQ subsystem to TSS:

TSS ADD(deptname) MQADMIN(ssid.)
TSS ADD(deptname) MQCMDS(ssid.)
TSS ADD(deptname) MQCONN(ssid.)
TSS ADD(deptname) MQNLIST(ssid.)

TSS ADD(deptname) MQPROC(ssid.)
TSS ADD(deptname) MQQUEUE(ssid.)

For V7.0.0 and above:

TSS ADD(deptname) MXADMIN(ssid.)
TSS ADD(deptname) MXNLIST(ssid.)
TSS ADD(deptname) MXPROC(ssid.)
TSS ADD(deptname) MXQUEUE(ssid.)
TSS ADD(deptname) MXTOPIC(ssid.)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

Another method to ensure protection is to assign the DEFPROT attribute to the resource class in the RDT record by using the following command:

TSS REP(RDT) RESCLASS(MQADMIN) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MQCMDs) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MQCONN) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MQNLIST) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MQPROC) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MQQUEUE) ATTR(DEFPROT)

For V7.0.0 and above:

TSS REP(RDT) RESCLASS(MXADMIN) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MXNLIST) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MXPROC) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MXQUEUE) ATTR(DEFPROT)
TSS REP(RDT) RESCLASS(MXTOPIC) ATTR(DEFPROT)

CCI: CCI-000213

CCI: CCI-002358

Group ID (Vulid): V-6960
Group Title: ZWMQ0051
Rule ID: SV-7539r3_rule
Severity: CAT I
Rule Version (STIG-ID): ZWMQ0051
Rule Title: Websphere MQ switch profiles must be properly 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.

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).

Automated Analysis requires Additional Analysis.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZWMQ0051)

b) Review the Security switches identified in response to the DISPLAY SECURITY command in each ssid report(s). If the all of the following switches specify ON, there is NO FINDING.

SUBSYSTEM
CONNECTION
COMMAND
CONTEXT
ALTERNATE USER
PROCESS
NAMELIST
QUEUE
COMMAND RESOURCES

c) If SUBSYSTEM specifies 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 COMMAND RESOURCE Security switch specify 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 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 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 profile permissions exist using the sample TSS command: TSS WHOHAS MQADMIN(ssid.NO) 2. Use the "TSS REVOKE(acid) MQADMIN(ssid.NO)" to revoke the permission.

CCI: CCI-000213

Group ID (Vulid): V-6962

Group Title: ZWMQ0052

Rule ID: SV-7542r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0052

Rule Title: WebSphere MQ MQCONN Class resources must be protected properly.

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.

Check Content:

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

- SENSITVE.RPT(WHOHMCON)

b) Review the following connection resources defined to the MQCONN resource class:

Resource Authorized Users

ssid.BATCH TSO and batch job ACIDs

ssid.CICS CICS region ACIDs

ssid.IMS IMS region ACIDs

ssid.CHIN Channel initiator ACIDs

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:

1) Access authorization restricts access to the appropriate users as indicated in (b) above.

- 2) All access FAILURES are logged.
- d) If all of the items in (c) are true, there is NO FINDING.
- e) If any 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 ACIDs
ssid.CICS CICS region ACIDs
ssid.IMS IMS region ACIDs
ssid.CHIN Channel initiator ACIDs

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:

- 1) Access authorization restricts access to the appropriate users as indicated in (b) above.
- 2) All access FAILURES are logged.

The following is a sample of the commands required to allow a batch user (USER1) to connect to a queue manager (QM1):

TSS ADD(USER1) FAC(QM1MSTR)
TSS PER(USER1) MQCONN(QM1.BATCH) ACC(READ)

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.

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

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.

Fix Text: The systems programmer responsible for supporting MQSeries/WebSphere MQ will ensure that the dead-letter queue and its alias are properly defined.

The following scenario describes how to securely define a dead-letter queue:

(1) Define the real dead-letter queue with attributes PUT(ENABLED) and GET(ENABLED).

(2) Give update authority for the dead-letter queue to CKTI (the MQSeries/WebSphere MQ-supplied CICS task initiator), channel initiators, and any automated application used for dead-letter queue maintenance.

(3) Define an alias queue that resolves to the real dead-letter queue, but give the alias queue the attributes PUT(ENABLED) and GET(DISABLED).

(4) To put a message on the dead-letter queue, an application uses the alias queue. The application does the following:

(a) Retrieve the name of the real dead-letter queue. To do this, it opens the queue manager object using MQOPEN, and then issues an MQINQ to get the dead-letter queue name.

(b) Build the name of the alias queue by appending the characters “.PUT” to this name, in this case, ssid.DEAD.QUEUE.PUT.

(c) Open the alias queue, ssid.DEAD.QUEUE.PUT.

(d) Put the message on the real dead-letter queue by issuing an MQPUT against the alias queue.

(5) Give the userid associated with the application update authority to the alias, but no access to the real dead-letter queue.

NOTE: If an alias queue is not used in place of the dead-letter queue, then the ACP rules for the dead-letter queue will be coded to restrict unauthorized users and systems from reading the messages on the file.

Undeliverable messages can be routed to a dead-letter queue. Two levels of access should be established for these queues. The first level allows applications, as well as some MQSeries / WebSphere MQ objects, to put messages to this queue. The second level restricts the ability to get messages from this queue and protects sensitive data. This will be accomplished by defining an alias queue that resolves to the real dead-letter queue, but defines the alias queue with the attributes PUT(ENABLED) and GET(DISABLED). The ability to get messages from the dead-letter queue will be restricted to message channel agents (MCAs), CKTI (MQSeries/WebSphere MQ-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-letter queue maintenance.

CCI: CCI-001762

Group ID (Vulid): V-6965

Group Title: ZWMQ0054

Rule ID: SV-7545r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0054

Rule Title: WebSphere MQ queue resource defined to the MQQUEUE 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.

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 report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(WHOHMQUE)

For all queue identified by the DISPLAY QUEUE(*) ALL command in the

MQSRPT(ssid). These queues will be prefixed by ssid to identify the resources to be protected. Ensure these queue resources are defined to the MQQUEUE resource class, if the following guidance is true, this is not a finding.

- 1) 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.
- 2) 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.
- 3) 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.*
- 4) 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.
- 5) 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 resource class, ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

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.

For system queues (i.e., ssid.SYSTEM.queueName), access authorization restricts access to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, and CICS regions running WebSphere MQ applications.

For the following system queues ensure that UPDATE access is restricted to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require

access to review message queues.

ssid.SYSTEM.COMMAND.INPUT
ssid.SYSTEM.COMMAND.REPLY
ssid.SYSTEM.CSQOREXX.*

For the following system queues (i.e., ssid.SYSTEM.CSQUTIL.*) ensure that UPDATE access is restricted to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors.

For the real dead-letter queue (to determine queue name refer to ZWMQ0053), 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.

For the alias dead-letter queue (to determine queue name refer to ZWMQ0053), 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.

NOTE: If an alias queue is not used in place of the dead-letter queue, then the RACF rules for the dead-letter queue will be coded to restrict unauthorized users and systems from reading the messages on the file.

The following is a sample of the commands required to allow a user (USER1) to get messages from or put messages to queues beginning with (PAY.) on subsystem (QM1):

TSS PER(USER1) MQQUEUE(QM1.PAY.) ACC(UPDATE)

Fix Text: For all queue resources defined to the MQQUEUE resource class, ensure the following items are in effect:

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 MQSRPT(ssid). These queues will be prefixed by ssid to identify the resources to be protected. Ensure these queue resources are defined to the MQQUEUE resource class, if the following guidance is true, this is not a finding.

1) 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.

2) 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.

3) 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.*

4) 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.

5) 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.

The following is a sample of the commands required to allow a user (USER1) to get messages from or put messages to queues beginning with (PAY.) on subsystem (QM1):

TSS PER(USER1) MQQUEUE(QM1.PAY.) ACC(UPDATE)

CCI: CCI-000213

Group ID (Vulid): V-6966

Group Title: ZWMQ0055

Rule ID: SV-7547r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0055

Rule Title: WebSphere MQ Process resources 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.

Check Content:

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

- SENSITIVE.RPT(WHOHMPRO)

b) For all process resources (i.e., ssid.processname) defined to 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: For all process resources (i.e., ssid.processname) defined to 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).

The following is a sample of the commands required to allow a user (USER1) to inquire on processes beginning with the letter V on queue manager (QM1):

```
TSS ADD(USER1) FAC(QM1MSTR)
TSS PER(USER1) MQPROC(QM1.V) ACC(READ)
ACTION(AUDIT)
```

CCI: CCI-000213

Group ID (Vulid): V-6967

Group Title: ZWMQ0056

Rule ID: SV-7549r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0056

Rule Title: WebSphere MQ Namelist resources 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.

Check Content:

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

- SENSITVE.RPT(WHOHMNLI)

b) For all namelist resources (i.e., ssid.namelist) defined to 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: For all namelist resources (i.e., ssid.namelist) defined to 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).

The following is a sample of the commands required to allow a user (USER1) to inquire on namelist TST1 on queue manager (QM1):

```
TSS ADD(USER1) FAC(QM1MSTR)
TSS PER(USER1) MQNLIST(QM1.TST1.) ACC(READ)
ACTION(AUDIT)
```

CCI: CCI-000213

Group ID (Vulid): V-6969

Group Title: ZWMQ0057

Rule ID: SV-7551r2_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.

Check Content:

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

- SENSITIVE.RPT(WHOHMADM)

b) For all alternate user resources (i.e., ssid.ALTERNATE.USER.alternatelogonid) defined to 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: For all alternate user resources (i.e., ssid.ALTERNATE.USER.alternateuserid) defined to 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).

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):

```
TSS ADD(USER1) FAC(QM1MSTR)
TSS PER(USER1) MQADMIN(QM1.ALTERNATE.USER.PS)
ACC(UPDATE) ACTION(AUDIT)
```

CCI: CCI-000213

Group ID (Vulid): V-6971

Group Title: ZWMQ0058

Rule ID: SV-7553r2_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: 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.

Check Content:

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

- SENSITIVE.RPT(WHOHMADM)

b) For all context resources (i.e., ssid.CONTEXT) defined to the 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: For all context resources (i.e., ssid.CONTEXT) defined to the 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).

The following is a sample of the commands required to allow a systems programming group (SYS1) to offload and reload messages for queue manager (QM1):

TSS ADD(SYS1) FAC(QM1MSTR)
TSS PER(SYS1) MQADMIN(QM1.CONTEXT) ACC(UPDATE) ACTION(AUDIT)

CCI: CCI-000213

Group ID (Vulid): V-6973
Group Title: ZWMQ0059
Rule ID: SV-7555r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZWMQ0059
Rule Title: WebSphere MQ command resources defined to MQCMDS 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.

Check Content:

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

- SENSITIVE.RPT(WHOHMCMD)

b) For all command resources (i.e., ssid.command) defined to 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, and all

profiles will be defined to the MQCMDS class.

For all command resources (i.e., ssid.command) defined to 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 table entitled "WebSphere MQ Command Security Controls " in the zOS STIG Addendum.

2) All command access is logged as designated in the table entitled "WebSphere MQ Command Security Controls " in the zOS STIG Addendum.

The following is a sample of the commands required to allow a systems programming group (SYS1) to issue the command CLEAR QLOCAL in subsystem QM1:

```
TSS ADD(SYS1) FAC(QM1MSTR)
TSS PER(SYS1) MQCMDS(QM1.CLEAR.LOCAL) ACC(ALTER)
      ACTION(AUDIT)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-6975
Group Title: ZWMQ0060
Rule ID: SV-7557r2_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: 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.

Check Content:

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

- SENSITIVE.RPT(WHOHMADM)

Automated Analysis

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

- PDI(ZWMQ0060)

b) Access authorization to these RESLEVEL resources restricts all access. No users are permitted access to ssid.RESLEVEL resources in the MQADMIN resource class.

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: 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.

In order to protect against any profile in the MQADMIN class, such as ssid.**, resolving to a RESLEVEL profile, an ssid.RESLEVEL permission will be created for each queue manager with an access of none.

The following sample command prevents access to ssid.RESLEVEL:

```
TSS PER(ALL) MQADMIN(ssid.RESLEVEL) ACCESS(NONE)
```

CCI: CCI-001762

UNCLASSIFIED