z/OS RACF STIG

Version: 8

Release: 12

13 Sep 2023

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

_____
Group ID (Vulid): V-223646
Group Title: CE000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): CE000010
Rule Title: Certificate Name Filtering must be implemented with appropriate
authorization and documentation.

Vulnerability Discussion: Certificate name filtering is a facility that allows
multiple certificates to be mapped to a single ACP userid. Rather than matching
a certificate stored in the ACP to determine the userid, criteria rules are

used. Depending on the filter criteria, a large number of client certificates
could be mapped to a single userid. Failure to properly control the use of
certificate name filtering could result in the loss of individual identity and
accountability.

Responsibility: Information Assurance Officer
IAControls: N/A

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

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

a) If certificate name filtering is in use, collect documentation
describing each active filter rule and written approval from the ISSM to use the
rule.

b) Issue the SETROPTS LIST command. If the DIGTNMAP resource class is
active, RACF is ready to process any certificate name filters with a Status of
TRUST. The DIGTNMAP resource class should not be active unless certificate name
filtering is desired.

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

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

RLIST DIGTNMAP *

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

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

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

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

d) If the DIGTNMAP resource class is active and certificate name filters
have a Status of TRUST, certificate name filtering is in use.

e) If certificate name filtering is in use and filtering rules have been
documented and approved by the ISSM, there is NO FINDING.

f) If certificate name filtering is in use and filtering rules have not
been documented and approved by the ISSM, this is a FINDING.

Fix Text: Ensure any certificate name filtering rules in use are documented and
approved by the ISSM.

Group ID (Vulid): V-223647
Group Title: CE000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): CE000020
Rule Title: Expired Digital Certificates must not be used.

Vulnerability Discussion: The longer and more often a key is used, the more
susceptible it is to loss or discovery. This weakens the assurance provided to a
relying Party that the unique binding between a key and its named subscriber is
valid. Therefore, it is important that certificates are periodically refreshed.
This is in accordance with DoD requirement. Expired Certificate must not be in
use.

Responsibility: N/A
IAControls: N/A

Check Content:
NOTE: The procedures in this checklist item presume the domain being reviewed is
running all releases of z/OS, and use the ACP as the certificate store.

The IAO will ensure that for production environments, expired certificates are
not used.

If the domain being reviewed is not a production system and is only used for
test and development, Expired Certificates review can be skipped.

RACDCERT ID(tcpip userid) LIST

a) 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.

b) 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-223699
Group Title: CE000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): CE000030
Rule Title: All digital certificates in use must have a valid path to a trusted
Certification authority.

Vulnerability Discussion: The origin of a certificate, the Certificate Authority (i.e., CA), is crucial in determining if the certificate should be
trusted. An approved CA establishes grounds for confidence at both ends of
communications sessions in ongoing identities of other parties and in the validity of information transmitted.

Responsibility: N/A
IAControls: N/A

Check Content:
NOTE: The procedures in this checklist item presume the domain being reviewed is
running all releases of z/OS, and use the ACP as the certificate store.

The IAO will ensure that for production environments, the list of Certificate
Authorities considered trusted by the Z/OS host are limited to those with a
trust hierarchy that leads to a DOD PKI Root Certificate Authority.

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.

RACDCERT ID(tcpip userid) LIST

a) 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.

b) If the digital certificate information indicates that the issuer's
distinguished name leads to a DoD PKI Root Certification Authority, External
Root Certification Authority (ECA), or an approved External Partner PKI s Root
Certification Authority, there is NO FINDING.

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-223649
Group Title: ES000010

Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000010
Rule Title: Write or greater access to SYS1.NUCLEUS must be limited to system
programmers only.

Vulnerability Discussion: This data set contains a large portion of the system
initialization (IPL) programs and pointers to the master and alternate master
catalog. Unauthorized access could result in the compromise of the operating
system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.NUCLEUS
1. Find the GAC field, if it shows a profile name (other than the Special
Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has
only been granted to system programming personnel, otherwise this is a
finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access
has only been granted to system programming personnel, otherwise this is
a finding.

b) Review the RACF Dataset List output for SYS1.NUCLEUS and check Audit
Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged
this is a finding.

c) If none of the above checks indicate a finding then there is NO
FINDING.

d) If any of the above checks indicate a finding then there 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-223650
Group Title: ES000020
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000020
Rule Title: Write or greater access to libraries that contain PPT modules must
be limited to system programmers only.

Vulnerability Discussion: Specific PPT designated program modules possess
significant security bypass capabilities. Unauthorized access could result in
the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:
a) Generate batch report JCL, as follows:.

1. From Analyzer main Menu, go to option 4
2. Press ENTER
3. Select option B - Sensitive/Critical Data Sets Analysis
4. Press ENTER
5. Select Link List Table (All libraries) by entering an S next to the prompt
6. At the bottom of the screen, select the following options as shown below:

Specify YES or NO to include the following:

AC(1) module list ===NO Duplicate Module Analysis ===NO
RACF detail ===YES Exceptions only ===NO
RACF Group detail ===YES
Search criteria ===NO
Sort criteria ===NO

7. Press ENTER

8. Select QG on the next panel, when the QG edit screen is displayed enter
the following beginning in column 2

```
LD DA('&DSNAME') VOLUME(&DSVOL) ALL
LD DA('&DSNAME') GEN ALL
```

9. Type ACCEPT at the Command line
10. Press ENTER
11. Select E on the JCL Submit Processing panel, when the generated JCL is
displayed modify the following:

```
//VSSQGOUT DD DSN=&&TEMPQG, UNIT=SYSALLDA,
// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),
// SPACE=(CYL,(1,1))
```

12. Add the following statements after the last generated JCL statement:

```
//STEP02 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)
```

b) Review the report output for all listed libraries,
1. Find the GAC field, if it shows a profile name (other than the Special Rule) with ACCESS other than NONE, this is a FINDING.
2. Find the UACC field, if access is other than NONE, this is a FINDING.
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.

c) Review the RACF Dataset List output for all listed libraries and check Audit
Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a FINDING.

d) If none of the above checks indicate a finding then there is NO FINDING.

e) If any of the above checks indicate a finding then there 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-235034
Group Title: ES000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000030
Rule Title: IBM RACF must limit WRITE or greater access to LINKLIST libraries 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 is 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 is used. Unauthorized access
could result in the compromise of the operating system environment, ACP, and
customer data.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100,
SRG-OS-000324-GPOS-00125

Responsibility: System Programmer
IAControls: N/A

Check Content:

From Any ISPF input line, enter:
TSO ISRDDN LINKLIST

If all of the following are untrue, this is not a finding.

If any of the following is true, this is a finding.

-The ACP data set rules for LINKLIST libraries do not restrict WRITE or greater
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) WRITE or greater access will be logged.

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.

Configure the WRITE or greater access to LINKLIST libraries to be limited to
system programmers only and all WRITER or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223652
Group Title: ES000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000040
Rule Title: Emergency USERIDs must be properly defined.

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

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

Check Content:
a) Refer to U_zOS_STIG_INSTRUCTION.doc., Preliminary Worksheet (Part 2 of 2),
Item 3:
Item 3: Copies of all source, vendor integrity statements, or other documentation
for all installed system, user, and ACP exits maintained by the site. Also
include
a list of the libraries in which these modules are contained.

b) To get DASDVOL, GDASDVOL Resource Class and Userid Information, do the following tasks:

1. Go to the Analyzer main menu, select option 4
2. On the Batch Reports menu select TSO UADS,option U
Note: Analyzer 8.1 with PTF VS48081 is required for this option to be available.
3. Press ENTER
4. Set Exceptions only and Sort Criteria fields to NO.
5. Press ENTER
6. On the JCL Submit Processing menu, select S to submit the batch report
7. Press ENTER
8. Go to the Administrator main menu, select Security Server Reports, option
3
9. On the Security Server Reports menu, select General Resource Profile, option 4.
a. On the General Resource reports screen:
b. Select Access Lists, option 4; and
c. Tab down to the Batch/Online prompt and enter B to generate a batch job; and
d. Tab to the Enhanced Masking prompt and enter Y next to it
e. Press ENTER

Note: You may need to be in extract mode to complete this. Type in extract at the command line, then <ENTER>, then enter the above screen.

10. On the Enhanced Masking panel enter the following masking string:
11. CLASS = DASDVOL OR CLASS=GDASDVOL
12. Press ENTER
13. On the Processing Options panel, enter Y by the prompt Explode RACF groups in access list after detail line
14. Press ENTER
15. On the JCL Submit Processing screen, select S to submit the batch job
16. Press ENTER
17. Return to the Security Server Reports menu, select User Profile, option 1
18. Press ENTER
19. On the User Reports screen, select User Summary, option 1
20. Tab down to the Batch/Online prompt and enter B to generate batch job
21. Press ENTER

22. On the JCL Submit Processing screen, select S to submit the batch job
23. Press ENTER
24. Ensure the following items are in effect regarding emergency userids:

a. Use the User Summary report to ensure userids exist to perform operating system functions without any RACF security administration privileges. These userids are defined to RACF with the system-OPERATIONS attribute, and FULL access to all DASD volumes. They must not have the SPECIAL attribute. Also, on the DASDVOL/GDASDVOL Access List report, ensure operating system function userids or any associated group are not in the access list of a resource profile.

NOTE: A user who has the system-OPERATIONS attribute has FULL access authorization to all RACF-protected resources in the DASDVOL/GDASDVOL resource classes. However, if their userid or any associated group (i.e., default or connect) is in the access list of a resource profile, they will only have the access specified in the access list.

b. Check the User Summary report to ensure userids exist to perform RACF security administration only. These userids are defined to RACF with the system-SPECIAL attribute. They must not have the OPERATIONS attribute.

c. On the User Summary report, ensure all emergency userids are defined to RACF. Use the TSO UADS Analysis report to ensure all emergency userids are defined to SYS1.UADS.

c) If all items (a,b,c) in (24) are true, there is NO FINDING.

d) If any item in (24) is untrue, this is a FINDING.

Fix Text: The IAO will review the emergency USERIDs to ensure access granted only authorizes those resources required to support the specific functions of either DASD Recovery or System Administration.

Ensure the following items are in effect regarding emergency userids:

At a minimum an emergency userids will exists with the security administration attributes specified in accordance with the following requirements:

- Userids exist to perform RACF security administration only. These userids are defined to RACF with the system-SPECIAL attribute. They must not have the OPERATIONS attribute. Emergency userids will have either SPECIAL or OPERATIONS but not both.

- Userids can be defined to perform operating system functions. Such userids must be defined without any RACF security administration privileges. These userids are defined to RACF with the system-OPERATIONS attribute, FULL access to all DASD volumes resources as well as the FACILITY Class STGADMN profiles. They must not have the SPECIAL attribute.

NOTE: A user who has the system-OPERATIONS attribute has FULL access authorization to all RACF-protected resources in the DASDVOL/GDASDVOL resource classes. However, if their userid or any associated group (i.e., default or connect) is in the access list of a resource profile, they will only have the access specified in the access list since access lists override OPERATIONS.

- Userids exist to perform RACF security administration only. These userids are defined to RACF with the system-SPECIAL attribute. They must not have the OPERATIONS attribute. Emergency userids will have either SPECIAL or OPERATIONS but not both.

- All emergency userids are defined to RACF and SYS1.UADS. See TSO Command Ref for info on adding users to UADS.

- All emergency userids are to be implemented with logging to provide an audit trail of their activities. This is accomplished with the UAUDIT attribute via the command:

ALU <uid> UAUDIT

- All emergency userids will have distinct, different passwords in SYS1.UADS and in RACF, 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 RACF.

- All emergency userids will have documented procedures - such as a COOP Plan - 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

userids is released for use, its password is to be reset by the IAO within 12
hours.

CCI: CCI-000035

CCI: CCI-001220

Group ID (Vulid): V-223653
Group Title: ES000050
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): ES000050
Rule Title: The SETROPTS LOGOPTIONS must be properly configured

Vulnerability Discussion: Audit records are central to after-the-fact investigations of security incidents. Every effort should be taken to collect as
much information as productively feasible for these investigative processes. The
SETROPTS LOGOPTIONS option serves as a default auditing requirement. Auditing
Failures as a minimum will assure a base level of information is available for
investigations.

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

Check Content:
a) In TSO Issue the SETR LIST command

b) Capture from the Screen all the CLASSES LISTED next to LOGOPTIONS
FAILURES CLASSES=

c) Capture from the Screen all the CLASSES LISTED next to ACTIVE=

d) If all ACTIVE classes are also listed under the LOGOPTIONS FAILURES
CLASSES= classes, there is NO FINDING

e) If any ACTIVE classes are not listed under the LOGOPTIONS FAILURES
CLASSES= classes, this is a FINDING.

f) LOGOPTIONS "NEVER" CLASSES = NONE is specified, then NO FINDING otherwise FINDING

Fix Text: Evaluate the impact associated with implementation of the control
option. Develop a plan of action to implement the control option as specified in
the example below:

CCI: CCI-000172

CCI: CCI-002234

Group ID (Vulid): V-223654
Group Title: ES000060
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000060
Rule Title: Memory and privileged program dumps must be protected in accordance
with proper security requirements.

Vulnerability Discussion: Access to memory and privileged program dumps running
Trusted Control Block (TCB) key 0-7 may hold passwords, encryption keys, or
other sensitive data that must not be made available. Failure to properly
control access to these facilities could result in unauthorized personnel
modifying sensitive z/OS lists. This exposure may threaten the integrity and
availability of the operating system environment, and compromise the
confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Note: Generic profiles can be used (i.e. IEA*.** below instead of IEAABD*) for
the checks below, as long as all the detailed requirements re access and logging
as specified below, are met.

Display profiles for the IEAABD. prefixed resources in the FACILITY resource
class as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER

e) On the General Resource Reports screen, select Access List, option 4
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Profile field and enter IEAABD*
h) Tab down to the Class field and enter FACILITY
i) Press ENTER
j) On the Processing Options panel, enter a Y next to Explode RACF groups in access list after detail line prompt
k) Press ENTER
l) On the JCL Submit Processing screen, select S to submit the batch job
m) Return to the General Reports screen , select Audit Flags, option 2
n) Tab down to the Batch/Online field, type a B (for batch)
o) Tab down to the Profile field and enter IEAABD*
p) Tab down to the Class field and enter FACILITY
q) Press ENTER
r) On the JCL Submit Processing screen, select S to submit the batch job
s) Review Access List report and Audit Flags report output and ensure that the following items are in effect:
1. IEAABD.** is defined with a UACC(NONE) and AUDIT(ALL)
2. IEAABD.DMPAUTH.** is defined with UACC(NONE) and SUCCESS(UPDATE) and FAILURES(UPDATE) or better specified. Only Systems Programmers are allowed UPDATE access. Anyone can have read access.
3. IEAABD.DMPAKEY.** is defined with a UACC(NONE), AUDIT(ALL) and access is limited to Systems Programming Personnel of READ or higher.
t) If any of the above in (s) is untrue for any of the specified IEAABD. resources, this is a FINDING.

Fix Text: Memory and privileged program dump resources are provided via resources in the FACILITY resource class. Ensure that the following are properly specified in the ACP.

(Note: The 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.

The RACF resource rules for the resources specify UACC(NONE) and NOWARNING.

Ensure that no access is given to IEAABD. resource.

Example

```
RDEF FACILITY IEAABD.** UACC(NONE) OWNER(owner group) AUDIT(ALL(READ))
```

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:

```
RDEF FACILITY IEAABD.DMPAUTH.** UACC(NONE) OWNER(owner group)
AUDIT(ALL(UPDATE))

PERMIT IEAABD.DMPAUTH.** CLASS(FACILITY) ID(authusers) ACCESS(READ)
PERMIT IEAABD.DMPAUTH.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
```

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

Example:

```
RDEF FACILITY IEAABD.DMPAKEY.** UACC(NONE) OWNER(owner group)
AUDIT(ALL(READ))

PERMIT IEAABD.DMPAKEY.** CLASS(FACILITY) ID(syspaudt) ACCESS(READ)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223655
Group Title: ES000070
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000070
Rule Title: z/OS system commands must be properly protected.

Vulnerability Discussion: z/OS system commands provide a method of controlling

the operating environment. Failure to properly control access to z/OS system
commands could result in unauthorized personnel issuing sensitive system commands. This exposure may threaten the integrity and availability of the
operating system environment, and compromise the confidentiality of customer
data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Display System Commands Controls in the OPERCMDS class as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER
e) On the General Resource Reports screen, select Access List, option 4
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Profile field and enter MVS*
h) Tab down to the Class field and enter OPERCMDS
i) Press ENTER
j) On the Processing Options panel, enter a Y next to Explode RACF groups in
access list after detail line prompt
k) Press ENTER
l) On the JCL Submit Processing screen, select S to submit the batch job
m) Return to the General Reports screen , select Audit Flags, option 2
n) Tab down to the Batch/Online field, type a B (for batch)
o) Tab down to the Profile field and enter MVS*
p) Tab down to the Class field and enter OPERCMDS
q) Press ENTER
r) On the JCL Submit Processing screen, select S to submit the batch job
s) Review Access List report and Audit Flags report output and ensure that the
following items are in effect:

1. On the Access List report, if the MVS.** resource is defined to the OPERCMDS class with a default access of NONE, there is NO FINDING.
On the Audit Flags report, if all failures and successes access to the MVS.** resource are logged, there is NO FINDING.

2. On the Access List report, if access to Z/OS system commands defined in the table entitled Reuired 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), 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.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

3. On the Audit Flag report, if all access (i.e., failures and successes) to specific Z/OS system commands is logged as indicated in the table entitled Controls on z/OS System Commands in the z/OS stig Addendum there is NO FINDING.

t) If any of the above in (s) is untrue for any Z/OS system command resource, this is a FINDING.

Fix Text: z/OS system commands provide control over z/OS functions and can compromise security if misused. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the z/OS system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when all less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

Apply the following recommendations when implementing security:

The MVS.** resource is defined to the OPERCMDS class with an access of NONE and all (i.e., failures and successes) access logged.

Access to z/OS system commands defined in the "Required Controls on z/OS System Commands" table in the zOS STIG Addendum is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

All access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled "Required Controls on z/OS System Commands" in the zOS STIG Addendum.

A sample set of commands to define and permit access to system command resources
is shown here:

```
RDEF OPERCMDS MVS.** UACC(NONE) OWNER(<syspaudt>) AUDIT(ALL(READ))
DATA("set up
deny-by-default profile per srr pdi acp00282')
```

Then, in accordance with the referenced table, use the following template to
define profiles for each command:

```
RDEF OPERCMDS <systemcommandprofile> UACC(NONE) OWNER(<syspaudt>)
AUDIT(ALL(READ))

PERMIT <systemcommandprofile> CLASS(OPERCMDS) ID(<groupname>)
ACCESS(<accesslevel>)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-223656
Group Title: ES000080
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000080
Rule Title: Users that have access to the CONSOLE resource in the TSOAUTH resource class are not properly defined.

Vulnerability Discussion: MCS consoles can be used to issue operator commands.
Failure to properly control access to MCS consoles could result in unauthorized
personnel issuing sensitive operator commands. This exposure may threaten the
integrity and availability of the operating system environment, and compromise
the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Display User CONSOLE and System Commands privilege information, as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER
e) On the General Resource Reports screen, select Access List, option 4
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Profile field and enter CONSOLE
h) Tab down to the Class field and enter TSOAUTH
i) Press ENTER
j) On the Processing Options panel, enter a Y next to Explode RACF groups in
access list after detail line prompt
k) Press ENTER
l) On the JCL Submit Processing screen, select S to submit the batch job
m) Press ENTER
n) Return to the Security Server Reports menu, select Profile reports, option 5
o) Press ENTER
p) On the Profile Reports menu, select OPERPARM, option 5 under User Segments.
q) Press ENTER
r) On the USER OPERPARM SEGMENT REPORT screen, tab down to the Batch/Online prompt and enter B for batch processing
s) Press ENTER
t) On the JCL Submit Processing screen, select S to submit the batch job
u) Press ENTER
v) Review Access List report for TSOAUTH class, User OPERPARM Segment report and Access List report for MVS* profiles in the OPERCMDS class generated in ACP00282, ensure the following are in effect:

1. On the class TSOAUTH Access List report, if the CONSOLE privilege is not defined to the TSOAUTH resource class, there is NO FINDING.

2. At the discretion of the IAO, users may be allowed to issues Z/OS system
commands from a TSO session. With this in mind, ensure the following items are in effect for users granted the CONSOLE resource in the TSOAUTH resource class:

a. On the User OPERPARM Segment report, ensure userids are restricted to the INFO level on the AUTH parameter specified in the OPERPARM segment of their userid, under the Console Authority field header.

b. On the OPERCMDS class Access List generated in ACP00282, ensure userids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the OPERCMDS resource class.

c. On the class TSOAUTH Access List generated above, ensure userids and/or group IDs are restricted to READ access to the CONSOLE resource defined in the TSOAUTH resource class.

If all of the above in (2) are true, there is NO FINDING.

If any of the above in (2) are untrue, this is a FINDING.

w) If all of the above in (v) are true, there is NO FINDING

x) If any of the above in (v) is untrue, this is a FINDING

Fix Text: Evaluate the impact of correcting any deficiencies. Develop a plan of
action and implement the required changes.
Ensure the following items are in effect for all MCS consoles:

1. Define a profile protecting the use of the CONSOLE command within TSO. A
sample command to accomplish this is shown here: RDEF TSOAUTH CONSOLE UACC(NONE)
OWNER(ADMIN) AUDIT(ALL(READ))

2. Permit only authorized users. A sample command to accomplish this is shown
here: PE CONSOLE CL(TSOAUTH) ID(<syspaudt>)

3. Set up the OPERPARM segment in corresponding user-class entry. A sample
command to accomplish this is shown here: ALU <authorizeduser> OPERPARM(AUTH(INFO))

4. Userids are restricted to READ access to the MVS.MCSOPER.userid resource
defined in the OPERCMDS resource class. A sample command to accomplish this is
shown here using the GLOBAL class:

```
 RDEF GLOBAL OPERCMDS ADDMEM(MVS.MCSOPER.&RACUID/READ) OWNER(ADMIN)
```

CCI: CCI-000213

Group ID (Vulid): V-223657
Group Title: ES000090
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000090
Rule Title: FACILITY resource class is inactive.

Vulnerability Discussion: IBM Provides the FACILITY Class for use in protecting
a variety of features/functions/products both IBM and third party. The FACILITY
Class is not dedicated to any one specific use and is intended as a
multi-purpose RACF Class. Failure to activate this class will result in

unprotected resources. This exposure may threaten the integrity of the operating
system environment, and compromise the confidentiality of customer data.

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

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
permission
bits and user audit bits for HFS objects that are part of the Z/OS UNIX Telnet
Server
component is configured according to the settings in the following table:

z/OS UNIX TELNET SERVER HFS OBJECT SECURITY SETTINGS
DIRECTORY or FILE PERMISSION BITS USER
AUDIT BITS
/usr/sbin/otelnetd 1740 fff
/etc/banner 0744 faf

a) Using Vanguard Administrator UNIX file manager option 14 open files browse
files above and review Permission bits and USER Audit bits.

b) If the HFS permission bits and user audit bits for each directory and file
match or
are more restrictive than the specified settings listed in the table above,
there is
NO FINDING.

NOTE: The /usr/sbin/otelnetd object is a symbolic link to /usr/lpp/tcpip/sbin/otelnetd.
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

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

Fix Text: The IAO will ensure that the FACILITY resource class is active.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
list of ACTIVE classes.

(1) The FACILITY Class is activated with the command SETR
CLASSACT(FACILITY).

(2) Generic profiles and commands should also be enabled with the command SETR
GENERIC(FACILITY) GENCMD(FACILITY).

(3) IBM recommends RACLISTing the FACILITY Class which is accomplished with the
command SETR RACL(FACILITY).

CCI: CCI-000213

Group ID (Vulid): V-223658
Group Title: ES000100
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000100
Rule Title: The OPERCMDS resource class is not active.

Vulnerability Discussion: z/OS system commands provide a method of controlling
the operating environment. Failure to properly control access to z/OS system
commands could result in unauthorized personnel issuing sensitive system
commands. This exposure may threaten the integrity and availability of the
operating system environment, and compromise the confidentiality of customer
data.

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

Check Content:
Display Resource Class Information as follows:

a) From Administrator main menu, select Security Server Commands,

b) Press ENTER

c) Select SETROPTS option 5 SETROPTS option,

d) Press ENTER

e) On the SETROPTS screen, locate the CDT Classes prompt, enter E next to it.

f) Press ENTER

g) Invoke the locate command, Locate OPERCMDS

h) Screen print the display showing the attributes of the OPERCMDS class, including active status
1. If the OPERCMDS class is ACTIVE there is NOFINDING
2. If the OPERCMDS class is not ACTIVE there is a FINDING

i) If Item 1 is true then there is NOFINDING

j) If Item 2 is true then there is a FINDING

Fix Text: The IAO will ensure that the OPERCMDS class is active.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
list of ACTIVE classes.

(1) The OPERCMDS Class is activated with the command SETR
CLASSACT(OPERCMDS).

(2) Generic profiles and commands should also be enabled with the command SETR
GENERIC(OPERCMDS) GENCMD(OPERCMDS).

(3) IBM recommends RACLISTing the OPERCMDS Class which is accomplished with the
command SETR RACL(OPERCMDS).

Refer to ACP00282 for information on content of the OPERCMDS class.

CCI: CCI-000213

Group ID (Vulid): V-223659
Group Title: ES000110
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000110
Rule Title: MCS consoles are not active.

Vulnerability Discussion: (RACF0248: CAT II) MCS consoles can be used to issue operator commands. Failure to properly control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

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

Check Content:
Display Resource Class Information as follows:

a) From Administrator main menu, select Security Server Commands,

b) Press ENTER

c) Select SETROPTS option 5 SETROPTS option,

d) Press ENTER

e) On the SETROPTS screen, locate the CDT Classes prompt, enter E next to it.

f) Press ENTER

g) Invoke the locate command, Locate OPERCMDS

h) Screen print the display showing the attributes of the OPERCMDS class, including active status
1. If the OPERCMDS class is ACTIVE there is NOFINDING
2. If the OPERCMDS class is not ACTIVE there is a FINDING

i) If Item 1 is true then there is NOFINDING

j) If Item 2 is true then there is a FINDING

Fix Text: The IAO will ensure that CONSOLE resource class is active.

Evaluate the impact associated with implementation of the control option.

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

The RACF Command SETR LIST will show the status of RACF Controls including a
list of ACTIVE classes.

(1) The CONSOLE Class is activated with the command SETR CLASSACT(CONSOLE).

(2) Generic profiles and commands should also be enabled with the command SETR
GENERIC(CONSOLE) GENCMD(CONSOLE).

(3) IBM recommends RACLISTing the CONSOLE Class which is accomplished with the
command SETR RACL(CONSOLE).

Refer to ACP00292, ACP00293, ACP00294 for information on content of the CONSOLE
class.

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223660
Group Title: ES000120
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000120
Rule Title: The CLASSACT SETROPTS must be specified for the TEMPDSN Class.

Vulnerability Discussion: CLASSACT specifies those classes defined by entries
in the class descriptor table for which RACF checking is to be ACTIVE. DATASET,
USER, and GROUP are active by default and cannot be activated or deactivated.

The system-wide options control the default settings for determining how the
Access Control Program (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.

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

Check Content:
Display Resource Class Information as follows:

a) In ISPF option #6, run SETR LIST

b) Press ENTER

c) Continue to press ENTERuntil the ACTIVE CLASSES heading appear, screen print
the area where the TEMPDSN classes is present.
1. If the class listed is active (i.e. in the ACTIVE CLASS list) , there is
NOFINDING
2. If any one of these classes listed are not active (i.e. Not in the ACTIVE
CLASS list), this is a FINDING

Fix Text: The IAO will ensure that SETROPTS CLASSACT has been specified, at
minimum, for the TEMPDSN resource class.

Evaluate the impact associated with implementation of the control option.
Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
list of ACTIVE classes.

IBM recommends activating the classes important to your installation. At minimum
the command:

SETR CLASSACT(TEMPDSN)

It is not recommended to perform a SETR CLASSACT(*).

CCI: CCI-000213

CCI: CCI-002262

Group ID (Vulid): V-223661
Group Title: ES000130
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000130
Rule Title: There are started tasks defined to RACF with the trusted attribute
that are not justified.

Vulnerability Discussion: Trusted Started tasks bypass RACF checking. It is
vital that this attribute is NOT granted to unauthorized Started Tasks which
could then obtain unauthorized access to the system. This could result in the
compromise of the confidentiality, integrity, and availability of the operating
system, ACP, or customer data.

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

Check Content:
a) Display STARTED class information as follows:
1. From Analyzer main Menu, go to option 3 - Online Displays
2. Press ENTER
3. Select option 4 - Started Procedures Analysis
4. Press ENTER

b) Review Started Procedures Analysis searching for STC definitions for the
following:
1. Review Started Procedures Analysis searching for STCs which show a
Yes under the PRI field heading. Use SORT PRI to sort any with a Y to
the bottom.
a. If any STC has a Y in the PRI column, there is a finding.
2. Next, Review the Started Procedures for any STC definitions with Y in the
TRU field (TRUSTED). Use SORT TRU on the command line to sort all
the trusted STC s to the bottom.
a. Validate that only STCs in the list below have the TRUSTED
attribute (ie, have a Y in the TRU column)
b. If additional STCs have the TRUSTED flag enabled, and
documentation exists from DISA Field Security Operations
approving the additional STCs, there is NO FINDING.
3. Ensure that an entry ** exists and has no access or resources granted to it
including a UACC of NONE.
a. To accomplish this go into ADMINISTRATOR, Option #4, On-
line Access and Authorization, fill in these fields with the specified

values and hit enter:
1. CLASS .. : STARTED
2. Resource Name (without quotes) . . **
3. Access to check . . . . . NONE
b. If the display field near the top left indicates that No Profile exists
(see b.1 below for an example) this is a finding as the ** profile must exist.
1. Profile: **No Profile exists**
c. On the screen that displays, CHECK that the UACC is NONE and that the ACCESS LIST that is displayed is NULL.
d. If any of the above is untrue, this is a FINDING..
c) If All Started Procedures conform with 1.a, 2.a & 2.b, 3.b & 3.c, there is NO
FINDING.
d) If any Started Procedure does not conform with1.a, 2.a & 2.b, 3.b & 3.c,,
there is
a FINDING.

TRUSTED STARTED TASKS
ACF2
ACFBKUP
APSWPROA
APSWPROB
APSWPROC
APSWPROM
APSWPROT
CATALOG
CONSOLE
DFHSM*
DFS
DUMPSRV
GPMSERVE
GSKSRVR
IEEVMPCR
IOSAS
IXGLOGR
JES2
JESXCF
LLA
NFS
OMVS/OMVSKERN***
RACF
RMF
RMFGAT
SMF
SMSRESTN
SMSRESTR
SMSVSAM
TCPIP
TSS
TSSB

TSSBKUP
TSSRESTN
VLF
VTAM
XCFAS
ZFS**

Fix Text: Review assignment of the TRUSTED attribute in ICHRIN03 and/or the
STARTED resource class. If a started proc defined with the TRUSTED attribute
exists that is not in the approved list of trusted started tasks as found in the
TRUSTED STARTED TASKS Table in the zOS STIG Addendum then the TRUSTED attribute
should be removed.

The TRUSTED attribute can be removed from a STARTED class profile using the
command:
RALT STARTED <profilename> STDATA(TRUSTED(NO))

If the STARTED class is RACLISTed then a refresh command is necessary:
SETR RACL(STARTED) REFRESH

If any Started Tasks exist with the PRIVILEGED attribute then take the following
action to remove this attribute:

RALT STARTED <profilename> STDATA(PRIVILEGED(NO))

If the STARTED class is RACLISTed then a refresh command is necessary:
SETR RACL(STARTED) REFRESH

CCI: CCI-000213

Group ID (Vulid): V-223662
Group Title: ES000140
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000140
Rule Title: The number of USERIDs possessing the Tape Bypass Label Processing
(BLP) privilege is not justified.

Vulnerability Discussion: BLP is extremely sensitive, as it allows the
circumvention of security access checking for the data. When BLP is used in
z/OS, the only verification that is done is for the data set name in the
JCL.

Any data set name can be used. A user could specify a data set name that he has
access to, the job would pass the validation check, and the job would be processed, giving access to the data. BLP is typically used for tapes that are
external to the tape management system used on the processor.

BLP should be granted to only a limited number of people, preferably the tape
librarian and a few key people from the operations staff. If an unauthorized
user possesses BLP authority, they could potentially read any restricted tape
and modify any information once it has been copied.

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

Check Content:
Display FACILITY class Bypass Label Processing (BLP) Information as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER
e) On the General Resource Reports screen, select Access List , option 4,
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Masking Fields area of the screen and enter ICHBLP by the
Profile field and FACILITY by the Class field
h) Press ENTER
i) On the JCL Submit Processing screen, select S to submit the batch job
j) Press ENTER
k) If no tape management system (e.g.CA 1) is installed, return to Administrator
main menu, select Security Server Commands, option 2, select SETROPTS
option 5, locate the CDT Edit prompt on the right hand side of the screen and
enter E, Press ENTER, on the next screen enter L TAPEVOL at the command
prompt, when the TAPEVOL information is displayed capture the screen.
l) Review General Resource Access List report output and ensure the following
items are in effect regarding bypass label processing (BLP):

1. The ICHBLP resource is defined to the FACILITY resource class with a UACC(NONE)
2. Access authorization to the ICHBLP resource is restricted at the userid
level to data center personnel (e.g. tape librarian, operations staff, etc.)
3. The number of userids authorized to the ICHBLP resource is not excessive.
4. If not tape management system (e.g., CA 1) is installed, the TAPEVOL

class is active (as shown on item (v) CDT screen capture)

m) If all items in (w) are true there is NOFINDING

n) If any item in (w) is untrue, this is a FINDING

Fix Text: Review all USERIDs with the BLP attribute. Ensure documentation providing justification for access is maintained and filed with the IAO, and
that unjustified access is removed.

BLP is controlled thru the FACILITY class profile ICHBLP. Access is removed with
the following command:
PE ICHBLP CL(FACILITY) id(<userid>) DELETE
a subsequent REFRESH of the FACILITY class may be required via the command: SETR
RACL(FACILITY) REFRESH

CCI: CCI-000213

Group ID (Vulid): V-223663
Group Title: ES000150
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000150
Rule Title: DASD Volume level protection does not exist or is improperly defined.

Vulnerability Discussion: Volume access grants default access to all data sets
residing on a given volume. This presents an exposure in the case of a data set
improperly placed on a volume or inappropriate access being granted to a volume.

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

Check Content:
Refer to the following items In U_zOS_STIG_INSTRUCTION.doc., Preliminary Worksheet (Part 2 of 2):

* Item 1
* Item 13

Display DASDVOL Information as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER

c) Select General Resource Profile, option 4,
d) Press ENTER
e) On the General Resource Reports screen, select Access List , option 4,
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Enhanced Masking prompt and enter Y
h) Press ENTER
i) On the Enhanced Masking edit panel, enter the following masking criteria:
CLASS=DASDVOL or CLASS=GDASDVOL
j) Press ENTER
k) On the JCL Submit Processing screen, select S to submit the batch job
l) Press ENTER
m) Review General Resource Access List report output and ensure the following
items are in effect regarding DASD volume controls:

1. A profile of * is defined to the DASDVOL resource class.
2. Access authorization to DASDVOL profiles is restricted to Storage Management Personnel, Storage Management Batch Userids, and Systems Programmers
3. All profiles defined to the DASDVOL resource class have UACC(NONE).

NOTE: Volume authorization allows access to all data sets on the volume, regardless of data set profile authorization. Access to operating system and general user storage volumes should be questioned. Refer to Section 3.3.2.5, Special Storage Management Users, and Section 3.3.2.6, Emergency Userids, in the Z/OS STIG for allowable usage of the DASDVOL/GDASDVOL resource classes.

n) If all items in (m) are true there is NOFINDING

o) If any item in (m) is untrue, this is a FINDING.

Fix Text: Develop a plan of action to implement the required changed.

1. Define profiles in the DASDVOL class. A sample command is provided here: RDEF
DASDVOL ** UACC(NONE) OWNER(<StgMgmtGrp>) AUDIT(ALL(READ)).

2. More specific DASDVOL profiles should be defined to protect groups of DASDVOLs. A sample command to create a profile protecting all DASDVOLs beginning
with "SYS" is provided here:
RDEF DASDVOL SYS* UACC(NONE) OWNER(<StgMgmtGrp>) AUDIT(ALL(READ)).

3. Permission can be granted to DASDVOL profiles. A sample command is provided
here: PE SYS* CLASS(DASDVOL) ID(<syspaudt>) ACCESS(ALTER)

4. If any profiles are in WARN Mode, they should be reset. A sample command is
provided here: RALT DASDVOL <profilenameNOWARN.

5. Note that the GDASDVOL class can also be used. See the RACF Security Admin
Guide for more info.

CCI: CCI-000213

Group ID (Vulid): V-223664
Group Title: ES000160
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000160
Rule Title: Sensitive Utility Controls will be properly defined and protected.

Vulnerability Discussion: Sensitive Utility Controls can run sensitive system
privileges or controls, and potentially can circumvent system and security
controls. Failure to properly control access to these resources could result in
the compromise of the confidentiality, integrity, and availability of the operating system environment, system services, ACP, and customer data.

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

Check Content:
a) In the Vanguard Administrator go to Option 3;4 which is Security Server
Reports; General Resource Profile and then make sure you are in LIVE MODE (type LIVE at the command line). choose O for ONLINE. In the Standard Masking Fields for CLASS: type in PROGRAM and hit ENTER. On the command line for each profile listed below type LR in the CMD line next to the
PROGRAM and PROFILE being checked:

b) If you Installation DOES NOT use MQSeries, this STEP B can be skipped.
1. Find the following classes in the output and validate that access is restricted per the Auth column in the Sensitive Utility Table in the Stig Addendum..

CSQUTIL
CSQUCVX
CSQJU003
CSQJU004
CSQ1LOGP

2. All Access is audited, e.g. ALL(READ)
a. If access is granted only as specified in the the Sensitive Utility Table and
audit is set to
ALL(READ) then there is NO FINDING.

b. If access is granted to anyone not specified in the Sensitive Utility Table
and audit is not
set to ALL(READ) then there is A FINDING.

c) Referring to the Sensitive Utility Table in the STIG Addendum, ensure that
all applicable programs or their generic
equivalents specified in the table meet the following requirements (e.g. ***GTF**,
***IOCP, *MASPZAP): Type LR next to each and ensure the following:
1. Profile is defined in the PROGRAM resource class.
2. Access is restricted to the appropriate personnel (e.g., systems programming, storage management, etc.) per the Auth column in the Sensitive
Utility Table in the Stig Addendum.
3. All access is audited, e.g., ALL(READ).
a. If all programs are defined, audited and with appropriate access, then there is NO FINDING
b. If any program is not defined, not audited or with inappropriate access, then there IS A FINDING

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 RACF resources as designated in the above table are defined with a default
access of NONE.

The RACF resource access authorizations restrict access to the appropriate
personnel as designated in the above table.

The RACF resource rules for the resources designated in the above table specify
UACC(NONE) and NOWARNING.

The following commands are provided as a sample for implementing resource controls:

```
RDEF PROGRAM AHLGTF ADDMEM('SYS1.LINKLIB'//NOPADCHK) -
DATA('ADDED PER SRR PDI RACF0770 ') -
AUDIT(ALL(READ)) UACC(NONE) OWNER(ADMIN)
PERMIT AHLGTF CLASS(PROGRAM) ID(stcgaudt)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-223665
Group Title: ES000170
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000170
Rule Title: RACF Global Access Checking must be restricted to appropriate classes and resources

Vulnerability Discussion: RACF Global access checking can be used to improve
the performance of RACF authorization checking for selected resources. The
global access checking table is maintained in storage and is checked early in
the RACF authorization checking sequence. If an entry in the global access
checking table allows the requested access to a resource, RACF performs no
further authorization checking. This can elimi

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

Check Content:
From a command input screen enter:
RL Global *

Alternately this can be viewed by following steps:
Refer to the following reports produced by the RACF Data Collection:

- DSMON.RPT(RACGAC)

Examine the Global Access Checking entries.

If Global * is specified in SETROPTS this is a finding.

The following entries may be allowed with the approval of the ISSM:
Dataset Class - ALTER access level to &RACUID.** (Allows users all access to
their own datasets)
OPERCMDS Class READ access to MVS.MCSOPER.&RACUID (Allows users access to console for their jobs)
JESJOBS Class ALTER access to CANCEL.*.*.&RACUID (Allows users to cancel their
own jobs)
JESJOBS Class ALTER access to SUBMIT.*.*.&RACUID (Allows users to submit their
own jobs)

The ISSM may allow other classes to be included after evaluation with the system
programmer.

If any other members are included for Global Access Checking this is a finding.

If written approval by the ISSM is not provided this is a finding.

Fix Text:
Ensure that Global Access Checking is appropriately administered.

Evaluate the impact associated with implementation of the control option.
Develop approval; documentation and a plan of action to implement the control
option as specified in the example below:
RALT GLOBAL class-name
ADDMEM (resourcename)/accesslevel)

CCI: CCI

CCI: CCI-000213

Group ID (Vulid): V-223666
Group Title: ES000180
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000180
Rule Title: Access greater than Read to the System Master Catalog must be limited to system programmers only.

Vulnerability Discussion: System catalogs are the basis for locating all files
on the system. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:
Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: Master Catalog Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for Master Catalog Name(s) and check
Audit Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the
impact of correcting the deficiency. Develop a plan of action and implement the
changes as required to protect the MASTER CATALOG.

The IAO will ensure that greater than READ access to MASTER CATALOG is limited
to system programmers only and all greater than READ access is logged.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223667
Group Title: ES000190
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000190
Rule Title: Write or greater access to SYS1.UADS must be limited to system
programmers only and read and update access must be limited to system programmer
personnel and/or security personnel.

Vulnerability Discussion: SYS1.UADS is the data set where emergency USERIDs are
maintained. This ensures that logon processing can occur even if the ACP is not
functional. Unauthorized access could result in the compromise of the operating
system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.UADS
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE or lower access is restricted to Systems Programming Personnel and/or Security Personnel. Verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE or lower access is restricted to Systems Programming Personnel and/or Security Personnel. Verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SYS1.UADS and check Audit Flag settings
1. If ALL failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223668
Group Title: ES000200
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000200
Rule Title: Dynamic lists must be protected in accordance with proper security
requirements.

Vulnerability Discussion: Dynamic lists provide a method of making z/OS system
changes without interrupting the availability of the operating system. Failure
to properly control access to these facilities could result in unauthorized
personnel modifying sensitive z/OS lists. This exposure may threaten the
integrity and availability of the operating system environment, and compromise
the confidentiality of customer data.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:
Display profiles for the CSV-prefixed resources in the FACILITY resource class
as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER

e) On the General Resource Reports screen, select Access List, option 4
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Profile field and enter CSV*
h) Tab down to the Class field and enter FACILITY
i) Press ENTER
j) On the Processing Options panel, enter a Y next to Explode RACF groups in
access list after detail line prompt
k) Press ENTER
l) On the JCL Submit Processing screen, select S to submit the batch job
m) Return to the General Reports screen , select Audit Flags, option 2
n) Tab down to the Batch/Online field, type a B (for batch)
o) Tab down to the Profile field and enter CSV*
p) Tab down to the Class field and enter FACILITY
q) Press ENTER
r) On the JCL Submit Processing screen, select S to submit the batch job
s) Review Access List report and Audit Flags report output and ensure that the
following items are in effect:

1. On the Access List report, if the following resources are defined with a UACC
(NONE), there is NO FINDING. On the Audit Flags report, if the following resources are defined with AUDIT(ALL), there is NO FINDING.

CSVAPF.**
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.**
CSVDYLPA.ADD.**
CSVDYLPA.DELETE.**
CSVDYNEX.**
CSVDYNEX.LIST
CSVDYNL.**
CSVDYNL.UPDATE.LNKLST
CSVLLA (include CSVLLA only if CICS is installed on your system).

2. On the Access List report, if access to all CSV-prefixed resources is restricted to only systems personnel, there is NO FINDING. In addition:
- Access to resource CSVLLA can include CICS userids and Control-O userids (if Control-O is installed on your system) in addition to systems programmers and there is NO FINDING
- READ access to resource CSVDYNEX.LIST is permitted to auditor userids and there is NO FINDING
- If any software product requires access to dynamic LPA updates on the system,
the RACF access to the CSVDYLPA resource and/or generic equivalent will be
defined with LOG and SERVICE(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.
 - If the products CA 1 and/or CA Common Services are on the system, the RACF
access to the CSVDYLPA.DELETE resource and/or generic equivalent will be defined
with AUDIT(ALL) and UPDATE access restricted to CA 1 and CA Common Services STC
userids.

Note: In the above, UPDATE access can be substituted with ALTER or CONTROL.
Review the permissions in the IBM documentation when specifying UPDATE

3. On the Audit Flags report, if all access to all CSV-prefixed resources is
 logged, there is NO FINDING.

t) If any of the above in (s) is untrue for any CSV-prefixed resource, this is a
 FINDING.

Fix Text: Ensure that the Dynamic List resources are defined to the FACILITY
resource class and protected. Only system programmers and a limited number of
authorized users and Approved authorized Started Tasks are able to issue these
commands. All access is logged.

The required CSV-prefixed Facility Class resources are listed below. These
resources or generic equivalents should be defined and permitted as required
with only z/OS systems programmers and logging enabled. Minimum required list of
CSV-prefixed resources:

CSVAPF.**
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.**
CSVDYLPA.ADD.**
CSVDYLPA.DELETE.**
CSVDYNEX.**
CSVDYNEX.LIST
CSVDYNL.**
CSVDYNL.UPDATE.LNKLST
CSVLLA.**

Limit authority to those resources to z/OS systems programmers. Restrict to the

absolute minimum number of personnel with AUDIT(ALL(READ)) and UPDATE access.

Sample commands are shown here to accomplish this:

```
RDEF FACILITY CSVAPF.** UACC(NONE) OWNER(syspaudt) AUDIT(ALL(READ))
RDEF FACILITY CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC.** UACC(NONE)
OWNER(syspaudt)
AUDIT(ALL(READ))
RDEF FACILITY CSVAPF.MVS.SETPROG.FORMAT.STATIC.** UACC(NONE)
OWNER(syspaudt)
AUDIT(ALL(READ))

PERMIT CSVAPF.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVAPF.MVS.SETPROG.SETPROG.FORMAT.DYNAMIC.** CLASS(FACILITY)
ID(syspaudt)
ACCESS(UPDATE)
PERMIT CSVAPF.MVS.SETPROG.SETPROG.FORMAT.STATIC.** CLASS(FACILITY)
ID(syspaudt)
ACCESS(UPDATE)
```

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

The CSVDYLPA.DELETE resource will be permitted to products CA 1 and CA Common
Services STC userids with AUDIT(ALL(READ)) and UPDATE access.

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

```
RDEF FACILITY CSVDYLPA.** UACC(NONE) OWNER(syspaudt) AUDIT(ALL(READ))
RDEF FACILITY CSVDYLPA.ADD.** UACC(NONE) OWNER(syspaudt) AUDIT(ALL(READ))
RDEF FACILITY CSVDYLPA.DELETE.** UACC(NONE) OWNER(syspaudt)
AUDIT(ALL(READ))

PERMIT CSVDYLPA.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(BMC Mainview STC userid)
ACCESS(UPDATE)
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(BMC Mainview STC userid)
ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.** CLASS(FACILITY) ID(CA 1 STC userid)
ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.** CLASS(FACILITY) ID(CCS STC userid)
ACCESS(UPDATE)
```

The CSVDYNEX.LIST resource and/or generic equivalent will be defined with

AUDIT(FAILURE(READ)SUCCESS(UPDATE)) 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:

```
RDEF FACILITY CSVDYNEX.** UACC(NONE) OWNER(syspaudt)
AUDIT(ALL(READ))
RDEF FACILITY CSVDYNEX.LIST.** UACC(NONE) OWNER(syspaudt)
AUDIT(FAILURE(READ)SUCCESS(UPDATE))

PERMIT CSVDYNEX.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVDYNEX.LIST.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVDYNEX.LIST.** CLASS(FACILITY) ID(audtaudt) ACCESS(READ)
```

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

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

```
RDEF FACILITY CSVLLA.** UACC(NONE) OWNER(syspaudt) AUDIT(ALL(READ))

PERMIT CSVLLA.** CLASS(FACILITY) ID(syspaudt) ACCESS(UPDATE)
PERMIT CSVLLA.** CLASS(FACILITY) ID(CICS STC userids) ACCESS(UPDATE)
PERMIT CSVLLA.** CLASS(FACILITY) ID(CONTROL-O STC userid) ACCESS(UPDATE)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-223669
Group Title: ES000210
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000210
Rule Title: Allocate access to system user catalogs are not limited to system
programmers only.

Vulnerability Discussion: System catalogs are the basis for locating all files

on the system. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:
Note: Refer to Set up for RACF Data Analysis.doc

a) Review the report output and locate Data set name: User Catalog Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for User Catalog Name(s) and check Audit
Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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.

The IAO will ensure that allocate access to USER CATALOGS are limited to system
programmers only and all allocate access is logged.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223670
Group Title: ES000220
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000220

Rule Title: Update and allocate access to System backup files are not limited to
system programmers and/or batch jobs that perform DASD backups.

Vulnerability Discussion: System backup data sets are necessary for recovery of
DASD resident data sets. Unauthorized access could result in the compromise of
the operating system environment, ACP, and customer data.

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

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: DASD Backup File Name(s)

1. Find the GAC field, if it shows a profile name (other than the Special Rule),
this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been
granted to system programming personnel and/or batch jobs that perform DASD
backups, otherwise this is a finding.

b) If none of the above checks indicate a finding then there is NO FINDING.

c) If any of the above checks indicate a finding then there 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-223671
Group Title: ES000230
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000230

Rule Title: Access to SYS(x).TRACE is not limited to system programmers only.

Vulnerability Discussion: SYS1.TRACE is used to trace and debug system problems. Unauthorized access could result in a compromise of the integrity and
availability of all system data and processes.

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

Check Content:
Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.TRACE
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify that READ or higher access has only been granted to system programming personnel and started tasks that perform GTF processing., otherwise this is a finding.
4. Under the Conditional Access list, verify that READ or higher access has
only been granted to system programming personnel and started tasks that perform GTF processing., otherwise this is a finding.

b) If none of the above checks indicate a finding then there is NO FINDING.

c) If any of the above checks indicate a finding then there 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-223672
Group Title: ES000240
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000240
Rule Title: RACF batch jobs are improperly secured.

Vulnerability Discussion: Batch jobs that are submitted to the operating system

should inherit the USERID of the submitter. This will identify the batch job
with a userid for the purpose of accessing resources. BATCHALLRACF ensures that
a valid USERID is associated with batch jobs. Jobs that are submitted to the
operating system via a scheduling facility must also be identified to the
system. Without a batch job having an associated USERID, access to system
resources will be limited.

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

Check Content:
Refer to the following item found in U_zOS_STIG_INSTRUCTION.doc, Preliminary
Worksheet (Part 2 of 2):

* Item 11
-
Display SURROGAT resource class information, as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER
e) On the General Resource Reports screen, select Access List, option 4
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Class field and enter SURROGAT
h) Press ENTER
i) On the Processing Options panel, enter a Y next to Explode RACF groups in
access list after detail line prompt
j) Press ENTER
k) On the JCL Submit Processing screen, select S to submit the batch job
l) Press ENTER
m) If the submission of batch jobs via an automated process (e.g. job scheduler,
job
submission started task, etc.) is being utilized, ensure the following items are
in
effect:

1.The SURROGAT resource class is active. Note: This does not need to
be checked, automation check is performed in ZUSSR060.

2. On the SURROGAT class Access List report, ensure each batch job
userid used for batch submission by a job scheduler (e.g., CONTROL-M,
CA-7, CA-Scheduler, etc.) is defined as an execution-userid in a
SURROGAT RESOURCE CLASS profile. For example:

```
 RDEFINE SURROGAT execution-userid.SUBMIT
 UACC(NONE) OWNER(execution-userid)
```

3. On the SURROGAT class Access List report, ensure each job scheduler useid (i.e. surrogate-userid) is permitted surrogate activity to the appropiate SURROGAT profiles. For example:

```
 PERMIT execution-userid.SUBMIT CLASS(SURROGAT)
 ID(surrogate-userid) ACCESS(READ)
```

n) If all of the above in (m) are true, there is NO FINDING

o) If any of the above in (m) is untrue, this is a FINDING

Fix Text: Ensure the following:

1. Each batch job userid used for batch submission by a job scheduler (e.g.,
CONTROL-M, CA-7, CA-Scheduler, etc.) is defined as an execution-userid in a
SURROGAT resource class profile. For example:

```
RDEFINE SURROGAT execution-userid.SUBMIT UACC(NONE)
OWNER(execution-userid)
```

2. Job scheduler userids (i.e., surrogate-userid) are permitted surrogate authority to the appropriate SURROGAT profiles. For example:

```
PERMIT execution-userid.SUBMIT CLASS(SURROGAT)
ID(surrogate-userid) ACCESS(READ)
```

CCI: CCI-000213

Group ID (Vulid): V-223673
Group Title: ES000250
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000250
Rule Title: RACF batch jobs are not protected with propagation control.

Vulnerability Discussion: Batch jobs that are user-submitted to the operating
system should inherit the USERID of the submitter. This will identify the batch
job with the user for the purpose of accessing resources. In some environments,
such as CICS, jobs submitted without the USER operand specified on the JOB
statement run under a user ID other than the user submitting the job, in this

case, the CICS userid. This situation presents a security violation in that the
issuer of the job will inherit the authority of the CICS userid.

The PROPCNTL Class was designed to prevent this from occurring. Utilize propagation control (PROPCNTL) for system-level address spaces that submit jobs
on behalf of users.

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

Check Content:
Refer to the following items found in U_zOS_STIG_INSTRUCTION.doc, Preliminary
Worksheet (Part 2 of 2):

* Item 9: List of all Multiple User Access Systems in use on this system. These
are systems that run in a single address space, but allow multiple users to sign
on to them (e.g., CICS regions, Session Managers, etc.). For each region, also
include corresponding userids, profiles, data management files, and a brief
description (of each region).

* Item 11: Documentation of the process used for submission of batch jobs via an
automated process (i.e., scheduler or other sources) and each of the associated
userids.

Display PROPCNTL Resource Class Information as follows:

a) From Administrator main menu, select Security Server Commands,
b) Press ENTER
c) Select SETROPTS (option 5),
d) Press ENTER
e) On the SETROPTS screen, locate the CDT Classes prompt, enter E next to it.
f) Press ENTER
g) At the command prompt, invoke the locate command for PROPCNTL, type L PROPCNTL
h) Screen print the display showing the attributes of the PROPCNTL class, including
active status
i) Return to the Administrator main menu and select Security Server Reports,
option
3
j) On the Security Server Reports menu, select General Resource Profile, option
4.

k) On the General Resource reports screen, select General Resource Profile
Summary, option 1
l) Enter Extract on the COMMAND line, Press ENTER
m) Tab down to the Batch/Online prompt and enter B to generate a batch job
n) Tab down to the Class field and enter PROPCNTL
o) Press ENTER
p) On the JCL Submit Processing screen, select S to submit the batch job
q) Press ENTER
r) If (1) the submission of batch jobs via an automated process (e.g. job scheduler,
job submission started task, etc.) is being utilized, and/or (2) Multiple User
Single
Address Space Systems (MUSASS) capable of submitting batch jobs are active
on this system, ensure the following items are in effect:

1. The PROPCNTL resource class is active, as displayed on the Security Server Commands CDT screen print.
2. On the class PROPCNTL General Resource Profile Summary report, ensure a PROPCNTL resource class profile is defined for each userid associated with a job scheduler (e.g. CONTROL-M, CA-7, etc.) and a MUSASS able to submit batch jobs (e.g., CA-ROSCOE, etc.)

s) If both of the above in (r) are true, there is NOFINDING

t) If either of the above in (r) is untrue, this is a FINDING

Fix Text: Add a PROPCNTL profile for each userid associated with a job scheduler
(e.g., CONTROL-M, CA-7, etc.) or a MUSASS able to submit batch jobs (e.g.,
CA-ROSCOE, etc.).

A sample command is shown here:
RDEF PROPCNTL controlm UACC(NONE) OWNER(ADMIN)

CCI: CCI-000213

Group ID (Vulid): V-223674
Group Title: ES000260
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000260
Rule Title: Write or greater access to SYS1.IMAGELIB must be limited to system
programmers only.

Vulnerability Discussion: SYS1.IMAGELIB is a partitioned data set containing
universal character set (UCS), forms control buffer (FCB), and printer control
information. Most IBM standard UCS images are included in SYS1.IMAGELIB during
system installation. This data set should be protected as a z/OS system data
set.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.IMAGELIB
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SYS1.IMAGELIB and check Audit Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there is a FINDING.

Fix Text: The IAO must ensure that UPDATE and/or ALLOCATE access to
SYS1.IMAGELIB is limited to system programmers only and all update and allocate
access is logged.

Review access authorization to critical system files. Evaluate the impact of
correcting the deficiency. Develop a plan of action and implement the changes as
required to protect SYS1.IMAGELIB.

SYS1.IMAGELIB is automatically APF-authorized. This data set contains modules,
images, tables, and character sets which are essential to system print services.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-223675
Group Title: ES000270
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000270
Rule Title: Write or greater access to SYS1.SVCLIB must be limited to system
programmers only.

Vulnerability Discussion: This data set is automatically APF-authorized, contains system SVCs, and may also contain I/O appendages. Unauthorized access
could result in the compromise of the operating system environment, ACP, and
customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.SVCLIB,
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SYS1.SVCLIB and check Audit Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there is a FINDING.

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-223676
Group Title: ES000280
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000280
Rule Title: Write or greater access to SYS1.LPALIB must be limited to system programmers only.

Vulnerability Discussion: SYS1.LPALIB is automatically APF-authorized during IPL processing and can contain SVCs. LPA modules, once loaded into the Link Pack Area, are capable of performing APF-authorized functions. This authorization allows a program to bypass various levels of security checking. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:
Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.LPALIB
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SYS1.LPALIB and check Audit Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there is a FINDING.

Fix Text: Review access authorization to critical system files. Evaluate the
impact of correcting the deficiency. Develop a plan of action and implement the
changes required to protect SYS1.LPALIB.

The IAO will ensure that update and allocate access to SYS1.LPALIB is limited to
system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-223677
Group Title: ES000290
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000290
Rule Title: Libraries included in the system REXXLIB concatenation must be
properly protected

Vulnerability Discussion: The libraries included in the system REXXLIB

concatenation can contain program modules which possess a significant level of
security bypass capability. Unauthorized access could result in the compromise
of the operating system environment, ACP, and customer data

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

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

SENSITVE.RPT(RACFREXX)

b) Verify that the REXXLIB datasets are properly restricted. If the following guidance is true, this is NOT A FINDING.
1) RACF data set access authorizations restrict Update or higher access to
z/OS systems programming personnel.
2) RACF data set access authorizations restrict READ to Appropriate Started Tasks, Auditors, and the AXRUSER, specified in the PARMLIB AXR00 AXRUSER().
3) All (i.e., failures and success) data set access authorities Update or
Higher is logged
4) RACF data set access authorizations specify UACC(NONE), that GAC is
either NONE or not specified, and NOWARNING.

c) If any of the above is untrue, 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.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-223678
Group Title: ES000300
Rule ID: N/A
Severity: CAT I

Rule Version (STIG-ID): ES000300
Rule Title: Write or greater access to all LPA libraries must be limited to
system programmers only.

Vulnerability Discussion: LPA modules, once loaded into the Link Pack Area, are
capable of performing APF-authorized functions. This authorization allows a
program to bypass various levels of security checking. Unauthorized access could
result in the compromise of the operating system environment, ACP, and customer
data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:
a) Generate batch report JCL, as follows:.
1. From Analyzer main Menu, go to option 4
2. Press ENTER
3. Select option B - Sensitive/Critical Data Sets Analysis
4. Press ENTER
5. Select LPA List Table by entering an S next to the prompt
6. At the bottom of the screen, select the following options as shown below:

Specify YES or NO to include the following:

AC(1) module list ===NO Duplicate Module Analysis ===NO
RACF detail ===YES Exceptions only ===NO
RACF Group detail ===YES
Search criteria ===NO
Sort criteria ===NO

7. Press ENTER
8. Select QG on the next panel, when the QG edit screen is displayed enter
the following beginning in column 2

```
LD DA('&DSNAME') VOLUME(&DSVOL) ALL
LD DA('&DSNAME') GEN ALL
```

9. Type ACCEPT at the Command line
10. Press ENTER
11. Select E on the JCL Submit Processing panel, when the generated JCL is
displayed modify the following:

```
//VSSQGOUT DD DSN=&&TEMPQG, UNIT=SYSALLDA,
// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),
// SPACE=(CYL,(1,1))
```

12. Add the following statements after the last generated JCL statement:

```
//STEP02 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)
```

b) Review the report output for all listed libraries,
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a FINDING.
2. Find the UACC field, if access is other than NONE, this is a FINDING.
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.

c) Review the RACF Dataset List output for all listed libraries and check Audit
Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

d) If none of the above checks indicate a finding then there is NO FINDING.
e) If any of the above checks indicate a finding then there 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. i

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-223679
Group Title: ES000310
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000310
Rule Title: Write or greater access to Libraries containing EXIT modules must be
limited to system programmers only.

Vulnerability Discussion: System exits have a wide range of uses and capabilities within any system. Exits may introduce security exposures within
the system, modify audit trails, and alter individual user capabilities. Unauthorized access could result in the compromise of the operating system
environment, ACP, and customer data.

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

Check Content:
Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: System Exit Lib Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for System Exit Lib Name(s) and check
Audit Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223680
Group Title: ES000320
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000320
Rule Title: Update and allocate access to all system-level product installation
libraries are not limited to system programmers only.

Vulnerability Discussion: System-level product installation libraries constitute the majority of the systems software libraries. Unauthorized access
could result in the compromise of the operating system environment, ACP, and
customer data.

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

Check Content:
note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SMP/E CSI Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SMP/E CSI Name(s) and check Audit
Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223683
Group Title: ES000350
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000350
Rule Title: Access to SYS1.LINKLIB is not properly protected.

Vulnerability Discussion: This data set is automatically APF-authorized, contains system SVCs and the base PPT. Unauthorized access could result in the
compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:

Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.LINKLIB,
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SYS1.LINKLIB and check Audit Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223684
Group Title: ES000360
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000360
Rule Title: The RACF System REXX IRRPWREX security data set must be properly

protected.

Vulnerability Discussion: The RACF System REXX named IRRPWREX contains sensitive access control and password information for the operating system environment and system resources. Unauthorized access could result in the compromise of passwords, the operating system environment, ACP (Access Control Program), and customer data.

Responsibility: Information Assurance Manager
IAControls: N/A

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

SENSITVE.RPT(RACFREXX)

OR

b) Refer to the zOS system REXXLIB concatenation found in SYS1. PARMLIB (AXR) for the data set that contains the REXX for Password exit named IRRPWREX and the defined AXRUSER.

c) Verify that the data set that contains IRRPWREX is properly restricted. If the following guidance is true, this is NOT A FINDING.
1) RACF data set access authorizations restrict READ to AXRUSER, z/OS systems programming personnel, security personnel, and auditors.
2 RACF data set access authorizations restrict UPDATE to security personnel using a documented change management procedure to provide a mechanism for access and revoking of access after use.
3) All (i.e., failures and success) data set access authorities (i.e., READ, UPDATE, and CONTROL) is logged
4) RACF data set access authorizations specify UACC(NONE) and NOWARNING.

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

Fix Text: Ensure that read access is restricted to security administrators, systems programmers, and auditors.
Ensure that there is a procedure documented with the ISSM that defines a change

management process to provide mechanism for granting Update access to security
administrators on an exception basis. The process should contain procedures to
revoke access when documented update is completed.
Ensure all failures and successes data set access authorities for RACF data set
that contains the Password exit is logged.

Examples:
ad 'sys3.racf.rexxlib.**' uacc(none) owner(sys3) -
 audit(all(read))
Permit 'sys3.racf.rexxlib.**' id(<syspaudt> <secaaudt> <audtaudt> AXRUSER)
acc(r)
Permit 'sys3.racf.rexxlib.**' id(<secaaudt>) acc(u)

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

CCI: CCI-002357

Group ID (Vulid): V-230209
Group Title: ES000365
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000365
Rule Title: The RACF System REXX IRRPHREX security data set must be properly
protected.

Vulnerability Discussion: The RACF System REXX named IRRPHREX contains sensitive access control and password information for the operating system
environment and system resources. Unauthorized access could result in the compromise of passwords, the operating system environment, ACP (Access Control
Program), and customer data.

Responsibility: Information Assurance Manager
IAControls: N/A

Check Content:

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

Collection:

SENSITVE.RPT(RACFREXX)

OR

b) Refer to the zOS system REXXLIB concatenation found in SYS1. PARMLIB (AXR)
for the data set that contains the REXX for Password exit named IRRPHREX and the
defined AXRUSER.

c) Verify that the data set that contains IRRPHREX is properly restricted. If
the following guidance is true, this is NOT A FINDING.
1) RACF data set access authorizations restrict READ to AXRUSER, z/OS systems
programming personnel, security personnel, and auditors.
2 RACF data set access authorizations restrict UPDATE to security personnel
using a documented change management procedure to provide a mechanism for access
and revoking of access after use.
3) All (i.e., failures and success) data set access authorities (i.e., READ,
UPDATE, and CONTROL) is logged
4) RACF data set access authorizations specify UACC(NONE) and NOWARNING.

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

Fix Text:
Ensure that read access is restricted to security administrators, systems programmers, and auditors.
Ensure that there is a procedure documented with the ISSM that defines a change
management process to provide mechanism for granting Update access to security
administrators on an exception basis. The process should contain procedures to
revoke access when documented update is completed.
Ensure all failures and successes data set access authorities for RACF data set
that contains the Password exit is logged.

Examples:

```
ad 'sys3.racf.rexxlib.**' uacc(none) owner(sys3) -
 audit(all(read))
Permit 'sys3.racf.rexxlib.**' id(<syspaudt> <secaaudt> <audtaudt>
AXRUSER)
acc(r)
Permit 'sys3.racf.rexxlib.**' id(<secaaudt>) acc(u)
```

CCI: CCI-000213

Group ID (Vulid): V-223685
Group Title: ES000370
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000370
Rule Title: The ACP security data sets and/or databases must be properly protected.

Vulnerability Discussion: The Access Control Program (ACP) database files
contain all access control information for the operating system environment and
system resources. Unauthorized access could result in the compromise of the
operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: RACF database Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), with ACCESS other than NONE, this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify READ access has
only been granted to Auditors, DASD Batch Jobs, system programming personnel,
security personnel,
and/or batch jobs that perform ACP maintenance, otherwise this is a finding.
4. Under the Conditional Access list, verify READ access
has only been granted toAuditors, DASD Batch Jobs, system programming personnel,
security
personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding.
5. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, security personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding.
6. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, security personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding.

NOTE: For RACF the dataset that contains the REXX for Password exit must be
included in these files. Examine system REXLIB concatenation for this dataset
name.

b) Review the RACF Dataset List output for RACF Database Name(s) and check
Audit Flag settings
1. If 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 not
logged this is a finding
c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there is a FINDING.

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-223686
Group Title: ES000380
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000380
Rule Title: Update and allocate access to data sets used to backup and/or dump

SMF collection files are not limited to system programmers and/or batch jobs
that perform SMF dump processing.

Vulnerability Discussion: SMF backup data sets are those data sets to which SMF
data has been offloaded in order to ensure a historical tracking of individual
user accountability. Unauthorized access could result in the compromise of the
operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SMF Dump/Backup Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel and batch job userids that perform SMF processing, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel and batch job userids that perform SMF processing, otherwise this is a finding.

b) Review the RACF Dataset List output for SMF Dump/Backup Name(s) and check
Audit Flag settings. Verify that Audit Successes is set to READ or UPDATE, and
Audit Failures is set to READ or UPDATE".
c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223687
Group Title: ES000390
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000390

Rule Title: All system PROCLIB data sets must be limited to system programmers
only

Vulnerability Discussion: Unauthorized access to PROCLIB data sets referenced
in the JES2 procedure can allow unauthorized modifications to STCs and other
system level procedures. This could result in the compromise of the operating
system environment, ACP, and customer data.

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

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: JES2 Proc Lib Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) If none of the above checks indicate a finding then there is NO FINDING.

c) If any of the above checks indicate a finding then there is a FINDING.

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 IEFPDSI 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.BRODCAST,DISP=SHR
```

JES2

```
//JES2 PROC
//IEFPROC EXEC PGM=HASJES20,PARM=NOREQ,
// DPRTY=(15,15),TIME=1440,PERFORM=9
//ALTPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2BKUP)
//HASPPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2PARM)
//PROC00 DD DSN=SYS3.PROCLIB,DISP=SHR <<===
// DD DSN=SYS2.PROCLIB,DISP=SHR <<===
// DD DSN=SYS1.PROCLIB,DISP=SHR <<===
//PROC01 DD DSN=SYS4.USERPROC,DISP=SHR
// DD DSN=SYS3.PROCLIB,DISP=SHR
// DD DSN=SYS2.PROCLIB,DISP=SHR
// DD DSN=SYS1.PROCLIB,DISP=SHR
//IEFRDER DD SYSOUT=*
//HASPLIST DD DDNAME=IEFRDER
```

JES2 initialization parameter JOBCLASS PROCLIB entries

```
JOBCLASS(*) ACCT=NO, /* ACCT # NOT REQUIRED (DEF.)*/

 PROCLIB=01, /* DEFAULT TO //PROC01 DD (DEF.)*/

JOBCLASS(STC) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/

 PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
```

```
JOBCLASS(TSU) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/

 PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
```

PROCLIB data set that will be used in the access authorization process:

SYS3.PROCLIB
SYS2.PROCLIB
SYS1.PROCLIB

The following PROCLIB data set will NOT be used or evaluated:

SYS4.USERPROC

Recommendation for sites:

The following are recommendations for the sites to ensure only PROCLIB data sets
that contain the STC and TSO procedures are protected.

- Remove all application PROCLIB data sets from MSTJCLxx and JES2 procedures. The customer will have all JCL changed to use the JCLLIB JCL statement to refer to the application PROCLIB data sets.

Example:

```
//USERPROC JCLLIB ORDER=(SYS4.USERPROC)
```

- Remove all access to the application PROCLIB data sets and only authorize system programming personnel WRITE and/or greater access to these data
sets.

- Document the application PROCLIB data set access for the customers that
require WRITE and/or greater access. Use this documentation as justification for
the inappropriate access created by the scripts.

- Change MSTJCLxx and JES2 procedure to identify STC and TSO PROCLIB data
sets separate from application PROCLIB data sets. The following is a list of
actions that can be performed to accomplish this recommendation:

a. Ensure that MSTJCLxx contains only PROCLIB data sets that contain STC
and TSO procedures.
b. If an application PROCLIB data set is required for JES2, ensure that
the JES2 procedure specifies more than one PROCxx DD statement concatenation or

identified in the JES2 dynamic PROCLIB definitions. Identify one PROCxx DD
statement data set concatenation that contains the STC and TSO PROCLIB data
sets. Identify one or more additional PROCxx DD statements that can contain any
other PROCLIB data sets. The concatenation of the additional PROCxx DD
statements can contain the same data sets that are identified in the PROCxx DD
statement for STC and TSO. The following is an example of the JES2 procedure:

```
//JES2 PROC
//IEFPROC EXEC PGM=HASJES20,PARM=NOREQ,
// DPRTY=(15,15),TIME=1440,PERFORM=9
//ALTPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2BKUP)
//HASPPARM DD DISP=SHR,
// DSN=SYS1.PARMLIB(JES2PARM)
//PROC00 DD DSN=SYS3.PROCLIB,DISP=SHR
// DD DSN=SYS2.PROCLIB,DISP=SHR
// DD DSN=SYS1.PROCLIB,DISP=SHR
//PROC01 DD DSN=SYS4.USERPROC,DISP=SHR
// DD DSN=SYS3.PROCLIB,DISP=SHR
// DD DSN=SYS2.PROCLIB,DISP=SHR
// DD DSN=SYS1.PROCLIB,DISP=SHR
//IEFRDER DD SYSOUT=*
//HASPLIST DD DDNAME=IEFRDER
```

c. Ensure that the JES2 configuration file is changed to specify that the
PROCLIB entry for the STC and TSU JOBCLASSes point to the proper PROCxx entry
within the JES2 procedure or JES2 dynamic PROCLIB definitions that contain the
STC and/or TSO procedures. All other JOBCLASSes can specify a PROCLIB entry that
uses the same PROCxx or any other PROCxx DD statement identified in the JES2
procedure or identified in the JES2 dynamic PROCLIB definitions. The following
is an example of the JES2 initialization parameters:

```
JOBCLASS(*) ACCT=NO, /* ACCT # NOT REQUIRED (DEF.)*/

 PROCLIB=01, /* DEFAULT TO //PROC01 DD (DEF.)*/

JOBCLASS(STC) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/

 PROCLIB=00, /* USE //PROC00 DD (DEF.)*/

JOBCLASS(TSU) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/

 PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
```

d. Ensure that only system programming personnel are authorized WRITE
and/or greater access to PROCLIB data sets that contain STC and TSO procedures.

CCI: CCI-000213

Group ID (Vulid): V-223688
Group Title: ES000400
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000400
Rule Title: Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) are
not limited to system programmers.

Vulnerability Discussion: Page data sets hold individual pages of virtual
storage when they are paged out of real storage. Unauthorized access could
result in the compromise of the operating system environment, ACP, and customer
data.

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

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: System Page Dataset(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify READ or higher access has only been granted to system programming personnel, otherwise this is a finding.

b) If none of the above checks indicate a finding then there is NO FINDING.

c) If any of the above checks indicate a finding then there 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-223689
Group Title: ES000410
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000410
Rule Title: MCS consoles access authorization(s) for CONSOLE resource(s) must be
properly protected.

Vulnerability Discussion: MCS consoles can be used to issue operator commands.
Failure to properly control access to MCS consoles could result in unauthorized
personnel issuing sensitive operator commands. This exposure may threaten the
integrity and availability of the operating system environment, and compromise
the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Display CONSOLE class information as follows:

a) From Analyzer main Menu
1. Go to option 3
2. Press ENTER
3. Select option L - Parmlib Analysis
4. Press ENTER
5. Press ENTERagain
6. On the next screen, look for entry CONSOLxx under the first LOADxx entry
7. Enter V next to CONSOLxx to view details
8. Press ENTER
9. Either save the information to another dataset or print the dataset directly.
10. Locate all console definitions by searching for NAME and noting each defined console name.

b) In Administrator
1. Select option 3 on the main menu
2. Press ENTER
3. Select General Resource reports, option 4
4. Press ENTER
5. Enter Extract on the COMMAND line, Press ENTER
6. Select Access List report, option 4
7. Select the Batch option by changing the Batch/Online option to a B
8. Enter the value CONSOLE on the CLASS field prompt

9. Press ENTER
10. On the Processing Options panel enter Y on Explode RACF Groups in access list after detail line
11. Press ENTER
12. Select S on the JCL Submit Processing
13. Review report output and ensure the following items are in effect for all MCS consoles:
a. Each console defined in the CONSOLxx parmlib members is defined to RACF with a corresponding profile in the CONSOLE resource class.
b. Each CONSOLE profile is defined with UACC(NONE).
c. The userid associated with each console has READ access to the corresponding resource defined in the CONSOLE resource class.
d. Access authorization for CONSOLE resources restricts READ access to Z/OS systems programming personnel and/or operations staff.

c) If all of the above in step 13 are true, there is NO FINDING.

d) If any of the above in step 13 are untrue, this is a FINDING.

Fix Text: The IAO must ensure that all MCS consoles are defined to the CONSOLE resource class and READ access is limited to operators and system programmers.

Review the MCS console resources defined to z/OS and the ACP, and ensure they conform to those outlined below.

Each console defined in the CONSOLxx parmlib member is defined to RACF with a corresponding profile in the CONSOLE resource class. See the IBM zOS OPERATIONS AND PLANNNG guide for further information.

Each CONSOLE profile is defined with UACC(NONE). A sample command file to accomplish items #1 and #2 is shown here:

```
RDEF CONSOLE MMDMST UACC(NONE) OWNER(syspaudt)
RDEF CONSOLE MMD041 UACC(NONE) OWNER(syspaudt)
RDEF CONSOLE MMDSCN UACC(NONE) OWNER(syspaudt)
RDEF CONSOLE ** UACC(NONE) OWNER(syspaudt) DATA('** represents all consoles not specifically defined')
```

Do not permit any user or group access to the ** profile. If a new console is added to the CONSOLxx member of it will be covered by this profile and a subsequent error will display in the log which will allow identification of the

undefined console.

The userid associated with each console will have READ access to the corresponding resource defined in the CONSOLE resource class. A sample command
file to accomplish this is shown here:

Note that the actual console groupid & userids are defined as part of ACP00292.

```
PE MMDMST CL(CONSOLE) ID(mmdmst)
PE MMDSCN CL(CONSOLE) ID(mmdscn)
PE MMD041 CL(CONSOLE) ID(mmd041)
```

Access authorization for CONSOLE resources restricts READ access to operations
and system programming personnel. A sample command file showing a permission of
READ access for sysprogs and operators is shown here:

```
PE MMDMST CL(CONSOLE) ID(syspaudt operaudt)
PE MMDSCN CL(CONSOLE) ID(syspaudt operaudt)
PE MMD041 CL(CONSOLE) ID(syspaudt operaudt)
```

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

Group ID (Vulid): V-223690
Group Title: ES000420
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000420
Rule Title: Update and allocate access to the JES2 System data sets (e.g.,
Spool, Checkpoint, and Initialization parameters) are not limited to system
programmers only.

Vulnerability Discussion: The JES2 System data sets are a common repository for
all jobs submitted to the system and the associated printout and configuration
of the JES2 environment. Unauthorized access could result in the compromise of
the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer

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

Check Content:
Note: Refer to Set up for RACF Data Analysis found in U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: JES2 System Dataset Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for JES2 System Dataset Name(s) and
check Audit Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223691

Group Title: ES000430
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000430
Rule Title: IEASYMUP resource will be protected in accordance with proper security requirements.

Vulnerability Discussion: Failure to properly control access to the IEASYMUP resource could result in unauthorized personnel modifying sensitive z/OS symbolics. This exposure may threaten the integrity and availability of the operating system environment.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Note: Generic profiles can be used (i.e. IEA*.** instead of IEASYMUP.**) for the checks below, as long as all the detailed requirements re access and logging as specified below, are met.

Ensure the following are in affect:

a) A covering profile for IEASYMUP.** exists and is defined with UACC(NONE) and AUDIT is specified as SUCCESSES(UPDATE) and FAILURES(READ)
b) Only systems programmers, DASD Administrators and Tape Librarians are in the access list with UPDATE access or higher
c) To verify
1. From the Administrator Main Menu Choose Option 3;4 (Security Server Reports, General Resource Profiles)
2. Tab down to CLASS and enter FACILITY
3. Tab down PROFILE and enter IEA*
4) Find the covering profile for IEASYMUP.* and type LR next to it in the command line.
5) Review the output against the requirements in a. above...
d) If all of the above are TRUE, there is NO FINDING.
e) If either
- a covering profile is not found or
- audit logging per above (SUCCESSES (UPDATE), FAILURES(READ)) is not specified or
- personnel other than Systems Programmers, DASD Administrators or Tape Librarians have UPDATE or higher access
then , there is a FINDING..

Fix Text: The IAO will ensure that the System level symbolic resources are
defined to the FACILITY resource class and protected. UPDATE access to the
System level symbolic resources are limited to System Programmers, DASD
Administrators, and/or Tape Library personnel. All access is logged. Ensure the
guidelines for the resources and/or generic equivalent are followed.

Limit access to the IEASYMUP resources to above personnel with UPDATE and/or
greater access.

The following commands are provided as a sample for implementing resource
controls:

```
rdef facility ieasymup.* uacc(none) owner(admin) -
       audit(all(read)) -
      data('protected per acp00350')
rdef facility ieasymup.symbolname uacc(none) owner(admin) -
       audit(all(read)) -
      data('protected per acp00350')

pe ieasymup.symbolname cl(facility) id(<dasdaudt) acc(u)
pe ieasymup.symbolname cl(facility) id(<syspaudt) acc(u)
pe ieasymup.symbolname cl(facility) id(<tapeaudt) acc(u)
```

CCI: CCI-002234

Group ID (Vulid): V-98089
Group Title: ES000440
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000440
Rule Title: The JES(BATCHALLRACF) SETROPTS value is not set to JES(BATCHALLRACF).

Vulnerability Discussion: (RACF0380: CAT II) JES(BATCHALLRACF) specifies that
JES is to test for the presence of a USERID and password on the job statement or
for propagated RACF identification information for all 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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, page down to the UserID Options area and locate the JES(BATCHALLRACF) field prompt, under JES on the left hand side of the screen.

b) Screen print the display showing the value of the JES(BATCHALLRACF) attribute.
1. If the JES(BATCHALLRACF) IS SET TO y,
there is NO FINDING
2. If the JES(BATCHALLRACF) value is NOT SET to Y, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: The IAO will ensure that JES(BATCHALLRACF) SETROPTS value is set to
JES(BATCHALLRACF). This specifies that JES is to test for a userid and password
on the job statement or for propagated RACF identification information for all
batch jobs.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
status of JES BATCHALLRACF.

(1) JES BATCHALLRACF is activated with the command SETR
JES(BATCHALLRACF).

CCI: CCI-002233

Group ID (Vulid): V-223693
Group Title: ES000460
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000460
Rule Title: The JES(XBMALLRACF) SETROPTS value is not set to JES(XBMALLRACF).

Vulnerability Discussion: (RACF0400: CAT II) XBMALLRACF ensures that (assuming you have JES configured to support XBM jobs) any XBM job submitted by a user must have a RACF identity or the job will fail. This is used only in JES2.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, page down to the UserID Options area and locate the XBMALLRACF field prompt, under JES on the left hand side of the screen.

b) Screen print the display showing the value of the JES(XBMALLRACF) attribute.
1. If the JES(XBMALLRACF) value is set to Y, there is NO FINDING
2. If the JES(XBMALLRACF) value is not set to Y, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: The IAO will ensure that JES(XBMALLRACF) SETROPTS value is set to
JES(XBMALLRACF). This specifies that JES is set to test for a userid and password on the job statement or for propagated RACF identification information
for all jobs run under the execution batch monitor.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
status of JES-XBMALLRACF.

(1) XBMALLRACF is activated with the command SETR XBMALLRACF.

CCI: CCI-000764

CCI: CCI-002233

Group ID (Vulid): V-223694
Group Title: ES000470
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000470
Rule Title: The OPERAUDIT SETROPTS value is not set to OPERAUDIT.

Vulnerability Discussion: (RACF0420: CAT II) OPERAUDIT specifies whether RACF
is to log all actions, such as accesses to resources and commands, allowed only
because a user has the OPERATIONS or group OPERATIONS attribute.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, locate the OPERAUDIT field prompt, under Auditing Options on the left hand side of the screen.

b) Screen print the display showing the value of the OPERAUDIT attribute.
1. If the OPERAUDIT value is set to Y, there is NO FINDING
2. If the OPERAUDIT value is not set to Y, this is a FINING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: NOTE: The RACF AUDITOR attribute is required in order to specify SETROPTS OPERAUDIT and also to display the OPERAUDIT attribute with the SETROPTS LIST command.

The IAO will ensure that OPERAUDIT SETROPTS value is set to OPERAUDIT. This specifies that RACF logs all actions such as accesses to resources and commands for a user who has operations or group operations attribute.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ATTRIBUTES.

(1) Logging of all actions, such as accesses to resources and commands, allowed only because a user has the OPERATIONS or group-OPERATIONS attribute is activated with the command SETR OPERAUDIT.

CCI: CCI-002234

CCI: CCI-002262

Group ID (Vulid): V-223695
Group Title: ES000480
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000480
Rule Title: The PASSWORD(REVOKE) SETROPTS value specified is not in accordance
with security requirements.

Vulnerability Discussion: (RACF0450: CAT II) The IAO will ensure that PASSWORD(REVOKE) SETROPTS value is
set to 1 or 2. This value specifies the number of consecutive incorrect password
attempts RACF allows before it revokes the USERID on the next incorrect attempt.
If you specify REVOKE, ensure
INITSTATS are in effect.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Password Options area and
locate the REVOKE field prompt, on the left hand side of the screen.
6. On the SETROPTS screen, scroll down to the UserID Options area and
ensure that Initstats is set to Y

b) Screen print the display showing the value of the PASSWORD(REVOKE) attribute.
1. If the PASSWORD(REVOKE) value is set to either 1 or 2, and Initstats is set to Y, there is NO FINDING
2. If the PASSWORD(REVOKE) value is not set to either 1 or 2, or Initstats is set to N, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: The IAO will ensure that PASSWORD(REVOKE) SETROPTS value is set to 1 or 2. This specifies the number of consecutive incorrect password attempts RACF allows before it revokes the USERID on the next incorrect attempt. If you specify REVOKE, ensure INITSTATS are in effect.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD REVOKE.

(1) Setting the password REVOKE to 2 invalid attempts activated with the command SETR PASSWORD(REVOKE(2)).

CCI: CCI-000044

Group ID (Vulid): V-223696
Group Title: ES000490
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000490
Rule Title: The PASSWORD(REVOKE) SETROPTS value specified is not in accordance with security requirements.

Vulnerability Discussion: (RACF0450: CAT II) The IAO will ensure that PASSWORD(REVOKE) SETROPTS value is set to 1 or 2. This value specifies the number of consecutive incorrect password

attempts RACF allows before it revokes the USERID on the next incorrect attempt.
If you specify REVOKE, ensure
INITSTATS are in effect.

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

Check Content:

a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Password Options area and locate the REVOKE field prompt, on the left hand side of the screen.
6. On the SETROPTS screen, scroll down to the UserID Options area and
ensure that Initstats is set to Y

b) Screen print the display showing the value of the PASSWORD(REVOKE)
attribute.
1. If the PASSWORD(REVOKE) value is set to either 1 or 2, and Initstats is
set to Y, there is NO FINDING
2. If the PASSWORD(REVOKE) value is not set to either 1 or 2, or Initstats
is set to N, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text:
The IAO will ensure that PASSWORD(REVOKE) SETROPTS value is set to 1 or 2. This
specifies the number of consecutive incorrect password attempts RACF allows
before it revokes the USERID on the next incorrect attempt. If you specify
REVOKE, ensure INITSTATS are in effect.

Evaluate the impact associated with implementation of the control option.
Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including
PASSWORD REVOKE.

(1) Setting the password REVOKE to 2 invalid attempts activated with the command
SETR PASSWORD(REVOKE(2)).

CCI: CCI

CCI: CCI-002238

Group ID (Vulid): V-223697
Group Title: ES000500
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000500
Rule Title: SYS1.PARMLIB is not limited to only system programmers.

Vulnerability Discussion: SYS1.PARMLIB contains the parameters which control
system IPL, configuration characteristics, security facilities, and performance.
Unauthorized access could result in the compromise of the operating system
environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SYS1.PARMLIB,
1. Find the GAC field, if it shows a profile name (other than the Special Rule) with an access other than NONE, this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify, that
a. READ access is restricted to System Level Started Tasks, Authorized Data Center Personnel, Auditors, Systems Programmers and Domain Level Security Administrators, otherwise this is a finding.
b. UPATE access is only granted to Systems Programming Personnel and/or Domain Level Security Administrators
c. ALTER access is only been granted to System Programming Personnel, otherwise this is a finding.

4. Under the Conditional Access list, verify, that
a. READ access is restricted to System Level Started Tasks, Authorized Data Center Personnel, Auditors, Systems Programmers and Domain Level Security Administrators, otherwise this is a finding.
b. UPATE access is only granted to Systems Programming Personnel

and/or Domain Level Security Administrators
c. ALTER access is only been granted to System Programming
Personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SYS1.PARMLIB and check Audit Flag
settings
1. If UPDATE and/or ALTER failures and successes are not being logged
this is a FINDING.

c) If none of the above checks indicate a finding then there is NO
FINDING.

d) If any of the above checks indicate a finding then there 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-223699
Group Title: ES000520

Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000520
Rule Title: The IBM RACF SETROPTS SAUDIT value must be specified.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

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

Check Content:

a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, locate the SAUDIT field prompt, on the left hand side of the screen under Auditing options.

b) Screen print the display showing the value of the SAUDIT attribute.
1. If the SAUDIT values is set to Y, there is NO FINDING
2. If the SAUDIT values is set to N, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there 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 as specified in the example below:

NOTE that in order to set or list the SAUDIT value, the RACF AUDITOR attribute is required. Reference the documentation for the SETROPTS command in the RACF Command Language Reference.

The RACF Command SETR LIST will show the status of RACF Controls including the
value for SAUDIT.

(1) SAUDIT is activated and set to the required value by issuing the command
SETR SAUDIT.

CCI: CCI

CCI: CCI-000172

Group ID (Vulid): V-223700
Group Title: ES000530
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): ES000530
Rule Title: The REALDSN SETROPTS value specified is improperly set.

Vulnerability Discussion: REALDSN specifies that RACF is to record, in any SMF
log records and operator messages, the real data set name (not the naming-conventions name) used on the data set commands and during resource
access checking and resource definition.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER

3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Dataset Options area and locate the REALDSN field prompt, on the right hand side of the screen.

b) Screen print the display showing the value of the REALDSN attribute.
1. If the REALDSN value is set to Y, there is NO FINDING
2. If the REALDSN value is not set to Y, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there 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 as specified in
the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the
value for the REALDSN Option.

(1) REALDSN is ACTIVATED by issuing the command SETR REALDSN.

CCI: CCI-001353

Group ID (Vulid): V-223701
Group Title: ES000540
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000540
Rule Title: Update and allocate access to SMF collection files (i.e., SYS1.MANx)
are not limited to system programmers and/or batch jobs that perform SMF dump
processing.

Vulnerability Discussion: SMF data collection is the system activity journaling
facility of the z/OS system. With the proper parameter designations it serves as
the basis to ensure individual user accountability. SMF data is the primary
source for cost charge back in DISA. Unauthorized access could result in the
compromise of logging and recording of the operating system environment, ACP,

and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:
Note: Refer to Set up for RACF Data Analysis found in
U_zOS_STIG_INSTRUCTION.doc.

a) Review the report output and locate Data set name: SMF Dataset Name(s)
1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
2. Find the UACC field, if access is other than NONE, this is a finding
3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.

b) Review the RACF Dataset List output for SMF Dataset Name(s) and check Audit
Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.

c) If none of the above checks indicate a finding then there is NO FINDING.

d) If any of the above checks indicate a finding then there 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-223702
Group Title: ES000550
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000550
Rule Title: The SETROPTS RVARYPW values will be properly set.

Vulnerability Discussion: RVARYPW specifies passwords that an operator is to use to respond with requests to approve RVARY command processing.

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.

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

Check Content:
a) Go to option TSO and execute a SETROPTS LIST

b) If the "INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT" message for both the SWITCH and STATUS functions and conforms to PASSWORD CONTENT requirements as documented in RACF0460, there is NO FINDING.

c) If the "INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT" message for both the SWITCH and STATUS functions but does not conform to PASSWORD CONTENT requirements as documented in RACF0460, this is a FINDING.

d) If the "DEFAULT RVARY PASSWORD IS IN EFFECT" message for the SWITCH or STATUS functions, this is a FINDING.

Fix Text: The IAO will ensure that the RVARYPW passwords are specified and
conform to password requirements documented in RACF0460. The IAO will evaluate
the impact associated with implementation of the control option and develop a
plan of action to implement the control option as required.

A sample command for setting both the SWITCH and STATUS passwords are shown
here:

SETR RVARYPW(SWITCH(Wxy$8Pqu) STATUS(pbZ0@wL2))

CCI: CCI-001813

Group ID (Vulid): V-223703
Group Title: ES000560
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000560
Rule Title: IBM RACF must define WARN = NO on all profiles.

Vulnerability Discussion: Failure to restrict system access to authenticated
users negatively impacts operating system security.

Responsibility: N/A
IAControls: N/A

Check Content:
a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select Data Set Profile, option 3 and General Resource Profile option 4
d) Press ENTER
e) On the Data Set Profile screen, select Warning Y
d) Press ENTER

Review all Dataset and resource profiles in the RACF database.

If any are not defined with WARN = NO, this is a finding.

Fix Text: Define each dataset and resource profile with WARN = NO
a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select Data Set Profile, option 3 and General Resource Profile option 4
d) Press ENTER
e) On the Data Set Profile screen, select Warning Y

d) Press ENTER
e) Enter VRC command and change Warning to N
f) Enter GO on command line
g) Eexecute VRAEXEC or VRABATCH or VRASCHED to make the change.

CCI: CCI-000366

Group ID (Vulid): V-223704
Group Title: ES000570
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000570
Rule Title: The PROTECTALL SETROPTS value specified is improperly set.

Vulnerability Discussion: When PROTECTALL processing is active and set to FAIL, the system automatically rejects any request to create or access a data set that is not RACF protected.

Temporary data sets that comply with standard MVS temporary data set naming conventions are excluded from PROTECTALL processing. PROTECTALL requires that data sets be RACF protected. In order for PROTECTALL to work effectively, you must specify GENERIC to activate generic profile checking. Otherwise, RACF would allow users to create or access only data sets protected by discrete profiles.

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.

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

Check Content:

Display Resource Class Information as follows:

a) From Administrator main menu, select Security Server Commands,
1. Press ENTER
2. Select SETROPTS option 5 SETROPTS option,
3. Press ENTER
4. On the SETROPTS screen, scroll down to the Dataset Options area and locate the PROTECTALL field prompt, on the left hand side of the screen.

b) Screen print the display showing the value of the PROTECTALL attribute.
1. If the SETROPTS PROTECTALL is set to PROTECTALL or PROTECTALL(FAILURE), there is NO FINDING.
2. If the SETROPTS PROTECTALL parameter is set to NOPROTECTALL or PROTECTALL(WARNING), this is a FINDING. Additional analysis may be required to determine whether this FINDING should be downgraded to a Category II or remain a Category I. Clear and specific documentation must be provided justifying the downgrade to a Category II.
a. Example of a Category I FINDING where no further analysis is required:
1. Control Options: SETROPTS NOPROTECTALL
b. Example of a possible Category I FINDING requiring additional analysis:
1. Control Options: SETROPTS PROTECTALL (WARNING). PROTECTALL(WARNING) allows access to a data set only if it is not protected by a profile in the DATASET resource class. Therefore if all sensitive data sets are properly protected by profiles in the DATASET resource class, PROTECTALL(WARNING) will not allow unauthorized access. This situation would justify a downgrade to a Category II.

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there 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 as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the value for the PROTECTALL Option.

(1) PROTECTALL is ACTIVATED and set to FAIL by issuing the command SETR PROTECTALL(FAIL).

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223705
Group Title: ES000580
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000580
Rule Title: The GRPLIST SETROPTS value is not set to ACTIVE.

Vulnerability Discussion: (RACF0350: CAT II) GRPLIST specifies that RACF processing is to perform group list access checking for all system users. When you specify GRPLIST, a users authority to access a resource is not based only on the authority of the users current connect group; access is based on the authority of any group to which the user is connected.

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.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, page down to the UserID Options area and locate the GRPLIST field prompt, on the right hand side of the screen.

b) Screen print the display showing the value of the GRPLIST attribute.
1. If the GRPLIST value is set to Y, there is NO FINDING
2. If the GRPLIST value is not set to Y, this is a FINDING

Fix Text: The IAO will ensure that GRPLIST SETROPTS value is set to ACTIVE.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
status of GRPLIST.

(1) List Of Groups Checking is activated with the command SETR GRPLIST.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223706
Group Title: ES000590
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000590
Rule Title: The RETPD SETROPTS value specified is improperly set.

Vulnerability Discussion: RETPD specifies the default RACF security retention
period for tape data sets. The security
retention period is the number of days that RACF protection is to remain in
effect for the
tape data set and should be set to a value of 99999.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Dataset Options area and locate the RETPD field prompt, on the left hand side of the screen.

b) Screen print the display showing the value of the RETPD attribute.
1. If the RETPD is set to 99999 (which means it never expires), there is NO
FINDING
2. If the RETPD is not set to 99999, this is a
FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there 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 as specified in
the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the
value for the RETPD (Retention Period) Option.

(1) RETPD is activated and set to the required value by issuing the command SETR
RETPD(99999).

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223707
Group Title: ES000600
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000600
Rule Title: The TAPEDSN SETROPTS value specified is improperly set.

Vulnerability Discussion: TAPEDSN activates tape data set protection. When tape
data set protection is

in effect, RACF can protect individual tape data sets as well as tape volumes.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Dataset options area and locate the TAPEDSN field prompt, on the right hand side of the screen.

b) Screen print the display showing the value of the TAPEDSN attribute.
1. If the TAPEDSN value is set to Y, there is NO FINDING
2. If the TAPEDSN value is set to N, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there 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 as specified in
the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the
value for the TAPEDSN Option.

(1) TAPEDSN is ACTIVATED by issuing the command SETR TAPEDSN.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223708
Group Title: ES000610
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000610
Rule Title: The WHEN(PROGRAM) SETROPTS value specified is not active.

Vulnerability Discussion: WHEN(PROGRAM) activates RACF program control, which includes both access control to load modules and program access to data sets.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Dataset options area and locate the PROGRAM field prompt, under WHEN on the left hand side of the screen.

b) Screen print the display showing the value of the WHEN(PROGRAM) attribute.
1. If the WHEN(PROGRAM) is set to Y, there is NO FINDING
2. If the WHEN(PROGRAM) values is not set to Y, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there 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 as specified in
the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the
value for the WHEN(PROGRAM) Option.

(1) WHEN(PROGRAM) is ACTIVATED by issuing the command SETR WHEN(PROGRAM).

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223709
Group Title: ES000620
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000620
Rule Title: The use of the RACF AUDITOR privilege is not justified.

Vulnerability Discussion: A user having the AUDITOR attribute has the authority
to specify logging options, gives control of logging SMF data and list auditing
information. With the AUDITOR attribute, a user could alter SMF logging data so
no trace of the activity could be found. This could destroy audit trace
information for the RACF system. This attribute should be limited to a minimum
number of people. This also applies to the use of Group-Auditor in cases where
users are connected to sensitive system dataset HLQ or general resource owning
groups with Group-Auditor.

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

Check Content:
Display User ID Information as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select User Profile, option 1,
d) Press ENTER
e) On the User Reports screen, select User Summary, option 1,
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Masking Fields area of the screen and enter Y next to the
Auditor
prompt
h) Press ENTER
i) On the JCL Submit Processing screen, select S to submit the batch job
j) Press ENTER
k) Review User Summary report output and ensure that the following items are in
effect regarding the AUDITOR attribute:

1. Authorization to the AUDITOR attribute is restricted to auditing and security personnel.
2. At minimum, ensure that any users connected to sensitive system dataset
HLQ groups or general resource owning groups with the Group-
AUDITOR attribute are Auditor and/or Security personnel. Otherwise, Group-AUDITOR is allowed

l) If both items in (k) are true there is NOFINDING

m) If either item in (k) is untrue, this is a FINDING

Fix Text: Review all USERIDs with the AU (Manual) - Review all USERIDs with the
AUDITOR attribute. Ensure documentation providing justification for access is
maintained and filed with the IAO, and that unjustified access is removed.

The AUDITOR attribute is removed from a user with the command: ALU <useridNOAUDITOR.

To remove the Group-Auditor attribute:

CO <user> GROUP(<groupname>) NOAUDITOR

CCI: CCI-000366

Group ID (Vulid): V-223710
Group Title: ES000630
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000630

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

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

Responsibility: Systems Programmer
IAControls: CODB-2, DCCS-1, DCCS-2

Check Content:
a) From Analyzer main Menu, go to 4;3. Specify NO for all options on the screen.
Submit the batch job and reference the report output. Review the RACF Databases
section of the report.

b) If the RACF database is not located on the same volume as either its alternate or
backup database, there is NO FINDING.

c) If the RACF database is located on the same volume as either its alternate or
backup database, 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-223711
Group Title: ES000640
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000640
Rule Title: ACP database is not backed up on a scheduled basis.

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

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

Check Content:
Refer to Vulnerability Questions within the SRRAUDIT Dialog Management
document.

a) If, based on the information provided, it can be determined that the RACF
database is being backed up on a regularly scheduled basis, there is NO
FINDING.

b) If it cannot be determined that the RACF 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-223712
Group Title: ES000650
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000650
Rule Title: Batch job user Ids must be properly defined.

Vulnerability Discussion: Batch jobs are submitted to the operating system
under their own USERID. This will identify the batch job with the user for the
purpose of accessing resources. BATCHALLRACF ensures that a valid USERID is
associated with batch jobs. Jobs that are submitted to the operating system via
a scheduling facility must also be identified to the system. Without a batch job
having an associated USERID, access to system resources will be limited.

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

Check Content:
Refer to the following item found in U_zOS_STIG_INSTRUCTION.doc, Preliminary
Worksheet (Part 2 of 2):

* Item 11
-
Display SURROGAT resource class information, as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select General Resource Profile, option 4,
d) Press ENTER
e) On the General Resource Reports screen, select Access List, option 4
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Class field and enter SURROGAT
h) Press ENTER
i) On the Processing Options panel, enter a Y next to Explode RACF groups in
access list after detail line prompt
j) Press ENTER
k) On the JCL Submit Processing screen, select S to submit the batch job

l) Press ENTER
m) If the submission of batch jobs via an automated process (e.g. job scheduler,
job
submission started task, etc.) is being utilized, ensure the following items are
in
effect:

1.The SURROGAT resource class is active. Note: This does not need to be checked, automation check is performed in ZUSSR060.

2. On the SURROGAT class Access List report, ensure each batch job userid used for batch submission by a job scheduler (e.g., CONTROL-M, CA-7, CA-Scheduler, etc.) is defined as an execution-userid in a SURROGAT RESOURCE CLASS profile. For example:

```
RDEFINE SURROGAT execution-userid.SUBMIT
UACC(NONE) OWNER(execution-userid)
```

3. On the SURROGAT class Access List report, ensure each job scheduler useid (i.e. surrogate-userid) is permitted surrogate activity to the appropiate SURROGAT profiles. For example:

```
PERMIT execution-userid.SUBMIT CLASS(SURROGAT)
ID(surrogate-userid) ACCESS(READ)
```

n) If all of the above in (m) are true, there is NO FINDING

o) If any of the above in (m) is untrue, this is a FINDING

Fix Text: Ensure the following:

1. Associated USERIDs exist for all batch jobs and documentation authorizing
access to system resources is maintained and implemented.
2. Set up the userids with the RACF PROTECTED attribute. A sample RACF command
to accomplish is shown here: ALU <execution-useridNOPASSWORD NOOIDCARD.

CCI: CCI-000052

CCI: CCI-000724

CCI: CCI-000764

CCI: CCI-000804

Group ID (Vulid): V-223713

Group Title: ES000660
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000660
Rule Title: The use of the RACF SPECIAL Attribute is not justified.

Vulnerability Discussion: The SPECIAL user attribute allows full authorization to modify all profiles in the RACF database and allows the user to perform all RACF functions, except those requiring AUDITOR attributes. This privilege should be limited to the security group and administrators because of the extreme control that these users have. Users with this privilege can alter any profile or resource on the system and could also alter the audit trail information.

The Group-Special attribute allows decentralized RACF control of datasets and resources. In cases where the scope of authority granted to a Group-Special Administrator has an impact on system security, the IAO needs to be fully aware and approve its use.

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

Check Content:
Display User ID Information as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select User Profile, option 1,
d) Press ENTER
e) On the User Reports screen, select User Summary, option 1,
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Masking Fields area of the screen and enter Y next to the Special prompt
h) Press ENTER
i) On the JCL Submit Processing screen, select S to submit the batch job
j) Press ENTER
k) Return to the Security Server Reports menu, select Connect Reports, option 15
l) Press ENTER
m) On the Connect Reports screen, select Connect Summary, option 1
n) Tab down to the Batch/Online field, type a B (for batch)

o) Tab down to the Masking Fields are of the screen and enter Y next to the
Special
prompt.
p) Press ENTER
q) On the JCL Submit Processing screen, select S to submit the batch job
r) Press ENTER
s) Review User Summary and Connect Summary report output and ensure that the
following items are in effect regarding the SPECIAL and GROUP-SPECIAL attributes:

1. Authorization to the SPECIAL or GROUP-SPECIAL attribute is restricted to security personnel.
2. At minimum, ensure that any users connected to sensitive system dataset
HLQ groups with the Group-SPECIAL attribute are security personnel. Otherwise, Group-SPECIAL is allowed.

t) If both items in (s) are true there is NOFINDING

u) If either item in (s) is untrue, this is a FINDING

Fix Text: Review all USERIDs with the SPECIAL attribute. Ensure documentation
providing justification for access is maintained and filed with the IAO, and
that unjustified access is removed.

For the SYSTEM SPECIAL attribute:

A sample command for removing the SPECIAL attribute is shown here: ALU <useridNOSPECIAL.

For the GROUP SPECIAL attribute:

CO <user> GROUP(<groupname>) NOSPECIAL

CCI: CCI-000035

Group ID (Vulid): V-223714
Group Title: ES000670
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000670
Rule Title: Assignment of the RACF OPERATIONS attribute to individual userids is
not fully justified.

Vulnerability Discussion: A user possessing the OPERATIONS attribute has authorization to do maintenance operations on all RACF-protected data sets, tape
volumes, and DASD volumes except those where the access list specifically limits
the OPERATIONS user to a lower access authority than the operation requires.

Because the OPERATIONS and GROUP-OPERATIONS privileges allow widespread access
they should be limited to users documented with a valid requirement. Delegation
of GROUP-OPERATIONS processing to other personnel by site-defined Group Administrators is forbidden.

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

Check Content:
Display User ID Information as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select User Profile, option 1,
d) Press ENTER
e) On the User Reports screen, select User Summary, option 1,
f) Tab down to the Batch/Online field, type a B (for batch)
g) Tab down to the Masking Fields area of the screen and enter Y next to the

Operations prompt
h) Press ENTER
i) On the JCL Submit Processing screen, select S to submit the batch job
j) Press ENTER
k) Return to the Security Server Reports menu, select Connect Reports, option 15
l) Press ENTER
m) On the Connect Reports screen, select Connect Summary, option 1
n) Tab down to the Batch/Online field, type a B (for batch)
o) Tab down to the Masking Fields are of the screen and enter Y next to the
Operations prompt.
p) Press ENTER
q) On the JCL Submit Processing screen, select S to submit the batch job
r) Press ENTER
s) Review User Summary and Connect Summary report output and ensure that the
following items are in effect regarding the OPERATIONS and GROUP-OPERATIONS attributes:

1. Authorization to the OPERATIONS or GROUP-OPERATIONS
attribute is restricted to key systems personnel, such as individuals

responsible for continuing operations and emergency recovery.

2. At minimum, ensure that any users connected to sensitive system dataset HLQ groups with the Group-OPERATIONS are key systems personnel, such as individuals responsible for continuing operations, Storage Management, and emergency recovery. Otherwise, Group-OPERATIONS is allowed.

NOTE: For sites running below RACF 2.1, the OPERATIONS attribute may be granted to STCs that do not require full TRUSTED status.

t) 2. If both items in (s) are true there is NOFINDING

u) If either item in (s) is untrue, this is a FINDING

Fix Text: Review all USERIDs with the OPERATIONS attribute. Ensure documentation
providing justification for access is maintained and filed with the IAO, and
that unjustified access is removed.

A sample command to remove the OPERATIONS attribute from a userid is shown here:

ALU <useridNOOPERATIONS

To remove the Group-Operations attribute:

CO <user> GROUP(<groupname>) NOOPERATIONS

CCI: CCI-002262

Group ID (Vulid): V-223715
Group Title: ES000680
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000680
Rule Title: The system programmer will ensure that the CONSOLxx members are
properly configured.

Vulnerability Discussion: MCS consoles can be used to issue operator commands.
Failure to properly control access to MCS consoles could result in unauthorized
personnel issuing sensitive operator commands. This exposure may threaten the
integrity and availability of the operating system environment, and compromise
the confidentiality of customer data.

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

Check Content:
Refer to the following items in SRR REVIEW PROCEDURES, Preliminary Worksheet
(Part 1 of 2):
* Item 2

a) Display PARMLIB information as follows:
1. From Analyzer main Menu, go to option 3
2. Press ENTER
3. Select option L - Parmlib Analysis
4. Press ENTER
5. Press ENTERagain
6. On the next screen, look for entry CONSOLxx under the first LOADxx entry
7. Enter V next to CONSOLxx to view details
8. Press ENTER
9. Either save the information to another dataset or print the dataset directly.

b) Ensure the following items are in effect:

1. The CONSOLE statement for each console specifies AUTH(INFO).

NOTE: (a) The AUTH parameter is not valid for consoles defined withUNIT(PRT).(b) Specifying AUTH(MASTER) is permissible for the system console.

2. The CONSOLE statement for each console assigns a unique name using the NAME parameter.
3. The DEFAULT statement for each CONSOLxx member specifies LOGON(REQUIRED) or LOGON(AUTO).

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

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

Fix Text: The Systems programmer should use the following recommendations and
techniques to provide protection for MCS consoles:

Ensure that the DEFAULT statement specifies LOGON(REQUIRED) so that all operators are required to log on prior to entering z/OS system commands. At the
discretion of the IAO, LOGON(AUTO) may be used.

Ensure that each CONSOLE statement specifies an explicit console NAME. And that
AUTH(INFO) is specified, this also including extended MCS consoles. AUTH(MASTER)
may be specified for systems console.

CCI: CCI-000382

CCI: CCI-002234

Group ID (Vulid): V-223716
Group Title: ES000690
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000690
Rule Title: MCS console userid(s) will be properly protected.

Vulnerability Discussion: MCS consoles can be used to issue operator commands.
Failure to properly control access to MCS consoles could result in unauthorized
personnel issuing sensitive operator commands. This exposure may threaten the
integrity and availability of the operating system environment, and compromise
the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
Display CONSOLE userid information as follows:

a) From Analyzer main Menu
1. Go to option 3
2. Press ENTER
3. Select option L - Parmlib Analysis
4. Press ENTER
5. Press ENTERagain
6. On the next screen, look for entry CONSOLxx under the first LOADxx entry
7. Enter V next to CONSOLxx to view details
8. Press ENTER
9. Either save the information to another dataset or print the dataset directly.
10. Locate all console definitions by searching for NAME and noting each defined console name.

b) In Administrator
1. Select option 3 on the main menu
2. Press ENTER
3. Select User, option 1
4. Press ENTER
5. Select User Summary report, option 1
6. Select the Batch option by changing the Batch/Online option to a B
7. Select the Enhanced Masking option, enter Y

8. On the Enhanced Masking panel, enter the following string:

Userid = console1 or Userid = console2 or Userid = console3 ..

9. Press ENTER
10. Select S on the JCL Submit Processing
11. Press ENTER
12. Review report output and ensure the following items are in effect:
a. Each console defined in the CONSOLxx parmlib members is associated with a valid RACF userid.
b. Ensure that RACF console userids are defined as follows:
1. No special attributes (e.g., SPECIAL, OPERATIONS, etc.). If this is true there is NO FINDING.
2. The RACF default group is the appropriate console group profile. If this is true, there is NO FINDING.

c) In Administrator
1. Select option 3 on the main menu
2. Press ENTER
3. Select ID In Access List, option 17
4. Press ENTER
5. Enter U for ID Type and Console Userid for the ID field
6. Select the Batch option by changing the Batch/Online option to a B
7. Leave the Masking Fields of Profile and Class with an * in them. All profiles and classes will need to be searched for access.
8. Set the UACC and * flags to Y, at the bottom of the screen
9. Press ENTER
10. Review report output and ensure the following item is in effect:
a. Restricted from accessing all data sets and resources except MCS.MCSOPER.consolename in the OPERCMDS resource class and consolename in the CONSOLE resource class. If this is true, there is NO FINDING.

Note: Repeat steps (5) thru (10) for each console userid.

d) In Administrator
1. Select option 3 on the main menu
2. Press ENTER
3. Select User, option 1
4. Press ENTER
5. Select User Summary report, option 1
6. Select the Enhanced Masking option, enter Y
7. On the Enhanced Masking panel, enter the following string:

Userid = console1 or Userid = console2 or Userid = console3 ..

8. Press ENTER
9. Enter the BRB line command next to the first userid listed on the report and on the last userid listed on the report

10. Press ENTER
11. Save command output to a dataset or PDS for future reference; review generated RACF commands and ensure console userids have no accesses to interactive on-line facilities (e.g., TSO, CICS, etc); if this is true, there is NOFINDING

e) If all of the above in (b.12), (c.10) and (d.11) are true, there is NO FINDING.

f) If any of the above in (b.12), (c.10) and (d.11) are not true, this is a FINDING.

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 RACF userid.

Each console userid has no special privileges and/or attributes (e.g., SPECIAL, OPERATIONS, etc.).

Each console userid has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.).

Each console userid will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMDS resource class and consolename in the CONSOLE resource class.

Each console userid has the RACF default group that is an appropriate console group profile.

NOTE: If LOGON(AUTO) is specified in the currently active CONSOLxx parmlib member, additional access may be required. Permissions for the console userids and/or console group may be given with access READ to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resource.

NOTE: Execute the JCL in CNTL(IRRUT100) using the RACF console userids as

SYSIN input. This report lists all occurrences of these userids within the RACF
database, including data set and resource access lists.

Examples:
AG consautolog SUPGROUP(<syspaudt>) OWNER(<syspaudt>) -
DATA(' group for console userids for autolog processing ')

AG consnoautolog SUPGROUP(<syspaudt>) OWNER(<syspaudt>) -
DATA('group for console userids for no autolog processing')

AU consname NAME('CONSOLE USERID FOR consname') NOPASSWORD NOOIDCARD -
 DFLTGRP(consautolog) OWNER(consautolog) -
 DATA('ADDED TO SUPPORT THE CHANGE TO LOGON(AUTO) IN CONSOLXX')

PERMIT MVS.CONTROL.** CL(OPERCMDS) ID(consautolog) ACCESS(READ)
PERMIT MVS.DISPLAY.** CL(OPERCMDS) ID(consautolog) ACCESS(READ)
PERMIT MVS.MONITOR.** CL(OPERCMDS) ID(consautolog) ACCESS(READ)
PERMIT MVS.STOPMN.** CL(OPERCMDS) ID(consautolog) ACCESS(READ)

PERMIT consname CL(CONSOLE) ID(consname)

CCI: CCI-000382

CCI: CCI-002232

Group ID (Vulid): V-223717
Group Title: ES000700
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): ES000700
Rule Title: RACF users do not have the required default fields.

Vulnerability Discussion: Ensure that Every USERID is uniquely identified to
the system. Within the USERID record, the user's name, default group, the owner,
and the user's passdate fields are completed. This will uniquely identify each
user. If these fields are not completed for each user, user accountability will
become lost.

Every user will be identified to RACF via each user s unique userid profile. To
RACF, a user is
an individual (user), a started task, or a batch job. Every userid will be fully
identified within
RACF with the following fields completed:
NAME User s name

DFLTGRP Default group
OWNER User s profile owner
PASSWORD Password

RACF will automatically assign the default group as the password if a password
is not explicitly
coded. Assign a unique password to every userid to prevent unauthorized access
by a person
who knows the default group for a new userid.

Responsibility: N/A
IAControls: DCCS-1, DCCS-2

Check Content:
Display User ID Information as follows:

a) From Administrator main menu, select Security Server Reports.
b) Press ENTER
c) Select User Profile, option 1,
d) Press ENTER
e) On the User Reports screen, select User Summary, option 1,
f) Tab down to the Batch/Online field, type a B (for batch)
g) Press ENTER
h) On the JCL Submit Processing screen, select S to submit the batch job
i) Review User Summary report output and ensure that the following items are in
effect for all users including batch userids:

1. A completed NAME field that can either be traced back to a current DD2875 or a Vendor Requirement (example: A Started Task).
2. The presence of the DEFAULT-GROUP and OWNER fields.
3. The PASSDATE field is not set to N/A unless this user has the PROTECTED attribute
j) If (i) any of the above is untrue, this is a FINDING.

Fix Text: Review all USERID definitions to ensure required information is provided. Evaluate the impact of correcting the deficiency. Develop a plan of
action and implement the changes listed in this PDI. The following are sample
commands to correct this vulnerability:

1. Add a NAME to a userid with the command ALU <userid> NAME('lastname, firstname').

2. Every user will be assigned a default group by default. A sample command to
reassign a default group is shown here: ALU <userid>
DFLTGRP(<newdefaultgroup>).
You must first be connected to a group via the RACF CONNECT command before

making it a default group.

3. A PASSDATE field showing 00.000 indicates that a temporary password has been
assigned but the user has not logged in and set a permanent password. This could
indicate that a new userid was recently added or that a userid previously added
is unused and should be considered for deletion. The IAO should investigate and
determine if the userid should be deleted or that the new user should be contacted and told to login to set a permanent password.

CCI: CCI-000764

CCI: CCI-000804

Group ID (Vulid): V-223718
Group Title: ES000710
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000710
Rule Title: Interactive USERIDs defined to RACF must have the required fields
completed.

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

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

Check Content:
Note: Current DoD policy has changed requiring that the password change interval
be
at the most 60 days. Ensure that this is in effect.
Note: FTP only process and server to server userids may have
PASSWORD(NOINTERVAL) 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.

a) Ensure that PASS-INTERVAL is a value of 1 to 60 days.
1. From the Vanguard Administrator main menu enter 2;5 to enter Vanguard RACF Commands panel.
2. Scroll to the area marked Password Options and verify that interval is set

between 1 to 60 days inclusive.
3. From the Vanguard Administrator main menu enter 3;1 to enter the User Reports panel.
4. Enter Y in the enhanced masking field of this panel and press enter.
5. On the enhanced command line enter PWDINTERVAL GE 61 and press enter.
6. If any list results this is a FINDING. Indicates these user ids do not have a
password interval set from 1 to 60.

b) Ensure that the following items are in effect for Interactive users (non-batch only
or STC protected users):

1. No userid has the LAST-ACCESS field set to UNKNOWN.
a. From the Vanguard Administrator main menu enter 3;1.
b. Press enter at the User Summary panel to list all RACF defined user ids.
c. From the resulting display enter sort racinit on the command line and press enter. The display will be sorted in descending order.

c) If a(6) list is blank, there is NO FINDING.

d) If a(6) list is not blank, this is a FINDING.

Fix Text: The IAO will review all interactive USERID definitions to ensure
required information is provided. Evaluate the impact of correcting any deficiencies. Develop a plan of action and implement the required changes.

The PASSWORD-INTERVAL for an interactive user must be set no higher than 60
days.

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

Note: FTP only process and server to server userids may have PASSWORD(NOINTERVAL) 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 or less.

A sample command to accomplish this is shown here:

PW USER(<userid>) INTERVAL(60).

The LAST-ACCESS date must be set to a valid date and not to the value UNKNOWN. A
sample command to accomplish this is shown here:

ALU <userid> RESUME

CCI: CCI-000199

CCI: CCI-000764

Group ID (Vulid): V-223719
Group Title: ES000720
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000720
Rule Title: Started Tasks are not properly identified to RACF.

Vulnerability Discussion: Started procedures have system generated job statements that do not contain the user, group, 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. If a USERID is not associated with the started procedure, the started procedure will not have access to the resources.

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

Check Content:
Refer to the following items found in U_zOS_STIG_INSTRUCTION.doc, Preliminary Worksheet (Part 1 of 2):

* Item 2

a) Display STARTED class information as follows:

1. From Analyzer main Menu, go to option 4
2. Press ENTER
3. Select option 4 - Started Procedures Analysis
4. Press ENTER
5. On the next screen, keep YES for Sort Criteria
6. Press ENTER
7. On the Sort Selection screen, enter a 1 next to the USERID field name This will list Started Procedure information in Userid order.
8. Press ENTER
9. On the JCL Submit Processing panel, select S to submit the job

b) Review Started Procedures Analysis Report output looking for userids associated

with multiple started procedures as well as started procedure names containing
an
* in the Procname, which indicates there might be multiple Started procedures
sharing this userid.

NOTE: For Vendor Products, STC userids are allowed to be unique per product and
function if supported by vendor documentation.

c) If all started task procedures have a unique associated userid, there is NO
FINDING.

d) If any started task procedure does not have a unique associated userid, this
is a
FINDING.

Fix Text: Define a RACF STARTED Class profile for each Started Proc that maps
the proc to a unique userid, or STC userids will be unique per product and
function if supported by vendor documentation. This can be accomplished with the
sample command:

RDEF STARTED <procname>.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
STDATA(USER(<userid>) GROUP(<groupname>) TRACE(YES))

A corresponding USERID must be defined with appropriate authority. The
"groupname" should be a valid STC group with no interactive users.

CCI: CCI-000764

Group ID (Vulid): V-223721
Group Title: ES000740
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000740
Rule Title: The Automatic Data Set Protection (ADSP) SETROPTS value is not set
to NOADSP.

Vulnerability Discussion: (RACF0250: CAT II) ADSP indicates that RACF
automatically creates discrete data set profiles to protect datasets created by
users having this attribute.

ADSP specifies that data sets created by users who have the ADSP attribute will
be RACF protected automatically. NOADSP cancels automatic RACF protection for
users who have ADSP.

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.

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

Check Content:
Display Resource Class Information as follows:

a) From Administrator main menu, select Security Server Commands,

b) Press ENTER

c) Select SETROPTS option 5 SETROPTS option,

d) Press ENTER

e) On the SETROPTS screen, locate the Dataset Options heading by using the PF8
key to scroll down the screen display

f) Screen print the display showing the ADSP attributes under the Dataset Options
heading, located on the right hand side of the screen.
1. If the ADSP value shows as N , there is NOFINDING
2. If the ADSP value shows as Y , this is a FINDING

Fix Text: The IAO will ensure that ADSP SETROPTS value is set to NOADSP.

Evaluate the impact associated with implementation of the control option.
Develop a plan of action to implement the control option as specified in the
example below:

NOADSP is set with the command SETR NOADSP.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223722
Group Title: ES000750
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000750
Rule Title: User accounts defined to the ACP do not uniquely identify system users.

Vulnerability Discussion: System users must be uniquely identified to the operating system. To accomplish this, each user must have an individual account defined to the ACP. If user accounts are not associated with specific individuals and are shared among multiple users, individual accountability is lost. This could hamper security audit activities and lead to unauthorized user access of system resources and customer data.
. Scope of, ownership of and responsibility over users shall be based upon the specifics of appointment, role, responsibilities and level of authority. Such as a domain/system level IAO is responsible for the Domain/system level users, whereas normally a application user would be the responsibility of the DoD AIS application security team unless SLA indicates otherwise.

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

Check Content:
The IAO will provide a list of all userids that are shared among multiple users(i.e not uniquely identified system users).

b) If there are no shared userids on this domain, there is NO FINDING.

c) If there are shared userids on this domain, this is a FINDING.

NOTE: Userids should be able to be traced back to a current DD2875 or a Vendor

Requirement (example: A Started Task).

Fix Text: The IAO wil identify user accounts defined to the ACP that are being
shared among multiple users. This may require interviews with appropriate
system-level support personnel. Remove the shared user accounts from the
ACP.

The IAO is required to uniquely identify each system user to the ACP, and that
access to resources is limited to those needed to perform the function. A user
is defined as either an individual accessing a computer resource, or as a task
executing on the system that requires access to a resource. On z/OS systems a
user is identified by means of a unique userid. Security requires that audit
data record the identity of the user, time of access, interaction with the
system, and sensitive functions that might permit a user or program to modify,
bypass, or negate security safeguards.
Any userid (user) on the system must be associated with only one individual also
any given individual may be assigned responsibility for multiple userids on a
given system, depending on functional responsibilities, to ensure task segregation.

CCI: CCI-000764

Group ID (Vulid): V-223723
Group Title: ES000760
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000760
Rule Title: The INACTIVE SETROPTS value is not set to 35 days.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, page down to the UserID Options area and locate the INACTIVE field prompt, on the right hand side of the screen.

b) Screen print the display showing the value of the INACTIVE attribute.
1. If the INACTIVE value is between 1 and 35, there is NO FINDING
2. If the INACTIVE value is 0 or greater then 35, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: The IAO will ensure that INACTIVE SETROPTS value is set to a value of
1 to 35 days, this specifies the number of days that a user is inactive and
still remain valid. INACTIVE specifies the number of days that a USERID can
remain unused and still be considered valid.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including a
status of INACTIVE.

The INACTIVE value is set properly with the command:

SETR INACTIVE(35)

CCI: CCI-000017

Group ID (Vulid): V-223724
Group Title: ES000770

Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000770
Rule Title: The PASSWORD(RULEn) SETROPTS value(s) 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 is, the greater the number of possible combinations that need to be tested before the password is compromised.
Use of a complex password helps to increase the time and resources required to compromise the password.

The PASSWORD SETROPTS value(s) specify the rules that RACF 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.

Responsibility: N/A
IAControls: N/A

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Password Options area and locate the RULE field prompt, on the right hand side of the screen.
6. Enter E next to the Rule field prompt to display Rule definitions.

b) Screen print the display showing the value of the PASSWORD(RULEn) attribute.
1. If the PASSWORD(RULEn) value conforms to at least one of the following:
RULE 1 LENGTH(8) $mmmmmmm
RULE 2 LENGTH(8) m$mmmmmm
RULE 3 LENGTH(8) mm$mmmmm
RULE 4 LENGTH(8) mmm$mmmm
RULE 5 LENGTH(8) mmmm$mmm
RULE 6 LENGTH(8) mmmmm$mm
RULE 7 LENGTH(8) mmmmmm$m
RULE 8 LENGTH(8) mmmmmmm$
there is NO FINDING

2. If the PASSWORD(RULEn) value does not conform to at least one of the above
rules,
this is a FINDING

c) If Item (b.1) is true then there is NO FINDING

d) If Item (b.2) is true then there is a FINDING

Fix Text: The ISSO will evaluate the impact associated with implementation of
the control option. Develop a plan of action to implement the control option as
specified in the example below:

For z/OS release 1.13 and 1.14 PTF UA90720 must be applied.
For z/OS Release 2.1 PTF UA90721 must be applied.

The RACF Command SETR LIST will show the status of RACF Controls including
PASSWORD SYNTAX RULEs.

Setting the password syntax to all Mixed Case Alphanumeric and Special Characters is activated with the commands:

```
setr password(mixedcase)
setr password(specialchars)
setr password(rule1(length(8) mixedall(1:8))
```

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000205

CCI: CCI-001619

Group ID (Vulid): V-223725
Group Title: ES000780
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000780
Rule Title: RACF exit ICHPWX01 must be installed and properly configured.

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

The RACF exit ICHPWX01 will allow for additional checks not available in RACF SETROPTS whenever 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.

Responsibility: N/A
IAControls: N/A

Check Content:
(assures that at least 1 upper 1 lower 1 number and 1 special character is used in Password)

The user's name cannot be contained in the password
Only 3 consecutive characters of the user's name are allowed
The minimum word length checked is 8

The user ID cannot be contained in the password
Only 3 consecutive characters of the user ID are allowed

Only 3 unchanged positions of the current password are allowed
These positions need to be consecutive to cause a failure
This check is not case sensitive

No more than 0 pairs of repeating characters are allowed
This check is not case sensitive

A minimum list of 33 restricted prefix strings is being checked:
APPL APR AUG ASDF BASIC CADAM DEC DEMO FEB FOCUS GAME IBM JAN JUL JUN LOG MAR MAY NET NEW NOV OCT PASS ROS SEP SIGN SYS TEST TSO VALID VTAM XXX 1234

If the modify command fails or returns the following message in the system log, this is a finding.

IRX0406E REXX exec load file REXXLIB does not contain exec member IRRPWREX.

Fix Text: Evaluate the impact associated with implementation of the control
option. Develop a plan of action to implement the control option as specified in
the example below:

For z/OS release 1.12 through z/OS release 2.1 APARs OA43998 and OA43999 must be
applied.

Install exit IRRPWREX according to instructions in z/OS Security Server RACF
System Programmer's Guide.

Note: RACF exit ICHPWX01 is coded to call a System REXX named IRRPWREX, so the
name cannot be changed without a corresponding change to ICHPWX01.

System REXX requires that this exec (IRRPWREX) reside in the REXXLIB concatenation.

Update parameters in IRRPWREX according to table Parameters for RACF IRRPWREX in
the z/OS STIG Addendum.

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000205

CCI: CCI-001619

Group ID (Vulid): V-230210
Group Title: ES000785
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000785
Rule Title: RACF exit IRRPHREX

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

Responsibility: N/A
IAControls: N/A

Check Content:

(assures that at least 1 upper 1 lower 1 number and 1 special character is used
in Password)

The user's name cannot be contained in the password
Only 3 consecutive characters of the user's name are allowed
The minimum word length checked is 8

The user ID cannot be contained in the password
Only 3 consecutive characters of the user ID are allowed

Only 3 unchanged positions of the current password are allowed
These positions need to be consecutive to cause a failure
This check is not case sensitive

No more than 0 pairs of repeating characters are allowed
This check is not case sensitive

A minimum list of 33 restricted prefix strings is being checked:
APPL APR AUG ASDF BASIC CADAM DEC DEMO FEB FOCUS GAME IBM JAN JUL
JUN LOG MAR MAY NET NEW NOV OCT PASS ROS SEP SIGN SYS TEST TSO
VALID VTAM XXX 1234

If the modify command fails or returns the following message in the system log,
this is a finding.

IRX0406E REXX exec load file REXXLIB does not contain exec member IRRPHREX.

Fix Text: Evaluate the impact associated with implementation of the control
option. Develop a plan of action to implement the control option as specified in
the example below:

For z/OS release 1.12 through z/OS release 2.1 APARs OA43998 and OA43999 must be
applied.

Install exit IRRPHREX according to instructions in z/OS Security Server RACF
System Programmer's Guide.

Note: RACF exit ICHPWX01 is coded to call a System REXX named IRRPHREX, so the
name cannot be changed without a corresponding change to ICHPWX01.

System REXX requires that this exec (IRRPHREX) reside in the REXXLIB concatenation.

Update parameters in IRRPHREX according to table Parameters for RACF IRRPWREX in
the z/OS STIG Addendum.

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000205

CCI: CCI-001619

Group ID (Vulid): V-223726
Group Title: ES000790
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000790
Rule Title: The PASSWORD(MINCHANGE) value will specified a value greater the
zero (0).

Vulnerability Discussion: MINCHANGE specifies the number of days that must pass
between a user s password and password phrase changes. Users can not change
their own passwords and password phrases within the minimum change 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.

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

Check Content:
a) Display the Password Minimum Change Interval Information as follows:

1. From Administrator main menu, select Security Server Commands, option 2.
2. Press Enter
3. From the VRC main menu, select SETROPTS option 5
4.. Press Enter
5. On the SETROPTS screen, scroll down to the Password Options area and locate
the MIN INTERVAL field prompt, on the right hand side of the screen

b) If the PASSWORD(MIN INTERVAL) greater than 0 and less than or equal to 59, there is NO FINDING
c) If the PASSWORD(MIN INTERVAL) value is 0 or greater than 59, this is a FINDING.

Fix Text: The IAO will ensure that PASSWORD(MINCHANGE) SETROPTS value number
from 1 to 59. This specifies the number of days that must pass before a user can
change their password.

Evaluate the impact associated with implementation of the control option.
Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including
PASSWORD MINCHANGE. Use the following command as an example command:

SETROPTS PASSWORD(MINCHANGE(1))

CCI: CCI-000198

Group ID (Vulid): V-223727
Group Title: ES000800
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000800
Rule Title: The PASSWORD(INTERVAL) SETROPTS value is not set to 60 days.

Vulnerability Discussion: (RACF0440: CAT II) INTERVAL specifies the maximum number of days that each users password is valid. When a user logs on to the system, RACF compares the system password interval value specified in the user profile. RACF uses the lower of the two values to determine if the users password has expired.

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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Password Options area and locate the INTERVAL field prompt, on the right hand side of the screen.

b) Screen print the display showing the value of the PASSWORD(INTERVAL) attribute.
1. If the PASSWORD(INTERVAL) value is less than or equal to 60 and not 0, there is NO FINDING

2. If the PASSWORD(INTERVAL) value is 0 or greater than 60, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: The IAO will ensure that PASSWORD(INTERVAL) SETROPTS value is set to
60 days. This specifies the maximum number of days that each user s password is
valid.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including
PASSWORD INTERVAL.

(1) Setting the password interval to 60 days is activated with the command SETR
PASSWORD(INTERVAL(60)).

CCI: CCI-000199

Group ID (Vulid): V-223728
Group Title: ES000810
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000810
Rule Title: The PASSWORD(HISTORY) SETROPTS value is not set to 10.

Vulnerability Discussion: (RACF0430: CAT II) HISTORY specifies the number of
previous passwords that RACF saves for each USERID and compares with an intended
new password. If there is a match with one of the previous passwords, or with
the current password, RACF rejects the intended new 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.

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

Check Content:
a) Display Resource Class Information as follows:
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, scroll down to the Password Options area and
locate the HISTORY field prompt, on the left hand side of the screen.

b) Screen print he display showing the value of the PASSWORD(HISTORY)
attribute.
1. If the PASSWORD(HISTORY) value is 10 or greater, there is NO FINDING
2. If the PASSWORD(HISTORY) value is not at least 10, this is a FINDING

c) If Item (b.1) is true then there is NO FINDING
d) If Item (b.2) is true then there is a FINDING

Fix Text: The IAO will ensure that PASSWORD(HISTORY) SETROPTS value is set to
10. This specifies the number of previous passwords that RACF saves for each
USERID and compares with an intended new password. If there is a match with one
of the previous passwords, or with the current password, RACF rejects the
intended new password.

Evaluate the impact associated with implementation of the control option.
Develop a plan of action to implement the control option as specified in the
example below:

The RACF Command SETR LIST will show the status of RACF Controls including
PASSWORD HISTORY.

(1) Setting the password history to 10 generations is activated with the command
SETR PASSWORD(HISTORY(10)).

CCI: CCI-000200

Group ID (Vulid): V-223729
Group Title: ES000820
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): ES000820
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.

Responsibility: N/A
IAControls: N/A

Check Content:
a) From the ISPF Command Shell enter

SETRopts List

OR

b) Refer to the following report(s) produced by the RACF Data Collection:

RACFCMDS.RPT(SETROPTS)
or
PDI(RACF0467) (Automated Analysis)

c) If the following is specified under PASSWORD PROCESSING OPTIONS:
THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES, this is not a Finding.

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:

For z/OS release 1.12 through z/OS release 2.1 APARs OA43998 and OA43999 must be
applied.

Set the passwords option for algorithm to KDFAES.

Sample syntax to activate:

SETRopts PASSWORD(ALGORITHM(KDFAES))

CCI: CCI-002450

Group ID (Vulid): V-223731
Group Title: ES000840
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000840
Rule Title: The ERASE ALL SETROPTS value must be set to ERASE(ALL) on all systems.

Vulnerability Discussion: The ERASE ALL specifies that data management is to erase all scratched data sets including temporary data sets. NOERASE specifies that no DASD data sets are erased when deleted.

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.

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

Check Content:
a) Display Resource Class Information as follows:.
1. From Administrator main menu, select Security Server Commands,
2. Press ENTER
3. Select SETROPTS option 5 SETROPTS option,
4. Press ENTER
5. On the SETROPTS screen, page down to the Dataset Options data area and locate the ERASE and ERASEALL field prompts.

b) Screen print the display showing the value of the ERASE and ERASEALL attributes.
1. For both CLASSIFIED and CONFIDENTIAL systems, if the ERASE value is set to Y, there is NO FINDING:

2. For UNCLASSIFIED systems, if the ERASE value is set to Y, there is NO FINDING:

c) For Classified and Confidential systems if b.1 is true there is NO FINDING,
otherwise FINDING
d) For Unclassified systems if b.2 is true there is NO FINDING, otherwise FINDING

Fix Text: The IAO must ensure that ERASE SETROPTS value is set to ERASE(ALL)
this allows DASD datasets to be erased when deleted.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the
example below:

- Issue the RACF Command SETR LIST to show the status of RACF Controls
including the status of the ERASE options.

- Take the appropriate actions to ensure that the SETR ERASE(ALL) has been
issued to enable Erase On Scratch for all datasets.

CCI: CCI-001090

Group ID (Vulid): V-223732
Group Title: ES000850
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): ES000850
Rule Title: Maintenance USERIDs are improperly controlled.

Vulnerability Discussion: DASD management USERIDs require access to backup and
restore all files, and present a high degree of risk to the environment. These
users should be given access to perform necessary functions thru use of the
DASDVOL class (for non-SMS volumes) and/or thru STGADMIN profiles in the FACILITY class for SMS managed volumes. Access to individual profiles in the
DATASET class should be disallowed. These userids should also set up IAW RACF0595 for batch userids which includes use of the PROTECTED Attribute.

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

Check Content:

a) Refer to U_zOS_STIG_INSTRUCTION.doc., Preliminary Worksheet (Part 2 of 2),
Item 1: for data required for this check.
* Item 1: All documents and procedures that apply to the following sections
and/or
units:
a. Operations Including system IPL procedures and SMF collection file backup specifics.
b. Storage Management Including identification of the DASD backup files and all associated storage management userids/LIDs/ACIDs.
c. Security Management and Tracking
d. Change Management

b) To display DASDVOL, GDASDVOL, FACILITY Resource Class and Userid Information, use Administrator for the following tasks:
1. Go to the Administrator Main Menu and select Security Server Reports, option 3
2. On the Security Server Reports menu, select General Resource Profile, option 4.
3. On the General Resource reports screen:
* Select Access Lists, option 4; and
* Tab down to the Batch/Online prompt and enter B to generate a batch job; and
* Tab to the Enhanced Masking prompt and enter Y next to it
* Press ENTER
Note: You may need to be in extract mode to complete this. Type in extract at
the command line, then <ENTER>, then enter the above screen.
4. On the Enhanced Masking panel enter the following masking string:

CLASS = DASDVOL OR CLASS=GDASDVOL

Note: If working with SMS-managed volumes, enter the following masking string instead:
CLASS=DASDVOL OR CLASS=GDASDVOL OR (CLASS=FACILITY
and PROFILE=STG*)

5. Press ENTER
6. On the Processing Options panel, enter Y by the prompt Explode RACF groups in access list after detail line
7. Press ENTER
8. On the JCL Submit Processing screen, select S to submit the batch job
9. Press ENTER
10. Return to the Security Server Reports menu, select User Profile, option 1
11. Press ENTER
12. On the User Reports screen:
* Select User Summary, option 1
* Tab down to the Batch/Online prompt and enter B to generate batch job
* Tab Down to the Operations masking field and overtype the * with a Y to list select userids with the operations attribute only
* Press ENTER

Note: You may need to be in extract mode to complete this. Type in extract at
the command line, then <ENTER>, then enter the above screen.

13. On the JCL Submit Processing screen, select S to submit the batch job
14. Press ENTER
15. Check the Access list report:

a) If batch userids assigned to storage maintenance tasks (e.g., volume backup, data set archive and restore, etc.) are given access to data sets using DASDVOL and/or GDASDVOL profiles, there is NO FINDING.

b) If working with SMS-managed volume, review access to FACILITY class, STG* profiles instead; if batch userids are given access to datasets
using FACILITY class, STG* profiles, there is NO FINDING.

NOTE: DASDVOL profiles will not work with SMS-managed volume. FACILITY class profiles must be used instead. If DFSMS/MVS is used to perform DASD maintenance operations, FACILITY class profiles may also be used to authorize storage maintenance operations to non-SMS-managed volumes in lieu of using DASDVOL profiles. Therefore, not all volumes may be defined to the DASDVOL/GDASDVOL resource classes, and not all storage management userids may be represented in the profile access lists.

16. Check the User Summary report. If any storage management userid is given the OPERATIONS attribute to perform DASD maintenance operations, this is a FINDING.
17. If the storage management userid is not defined with the PROTECTED attribute, this is a FINDING
18. If both of the above in (15) , (16) and (17) are true, there is NOFINDING
19. If either of the above in (15), (16) and (17) is untrue, this is a FINDING

Fix Text: Evaluate the impact of accomplishing the change. Develop a plan of
action and implement the change as required.

Ensure that storage management userids do not possess the OPERATIONS attribute.
A sample command to accomplish this is shown here: ALU <useridNOOPERATIONS

Ensure that storage management userids possess the PROTECTED attribute. A sample
command to accomplish this is shown here: ALU <useridNOPASS NOOIDCARD

Ensure that storage management userids are permitted to the appropriate STGADMIN
profiles in the FACILITY class for SMS-managed volumes.

Ensure that storage management userids are permitted to appropriate DASDVOL
profiles for non-SMS-managed volumes.

CCI: CCI-000213

Group ID (Vulid): V-223733
Group Title: FT000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000010
Rule Title: SMF recording options for the FTP Server must be configured to write
SMF records for all eligible events.

Vulnerability Discussion: The FTP Server can provide audit data in the form of
SMF records. The SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. Failure to collect and retain audit data may contribute to the loss of accountability and
hamper security audit activities.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECAT-1, ECAT-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the FTP
Server
FTP.DATA configuration statements are coded according to the settings in the
following
table

a) From the ISPF Primary Option Menu use option 3.4 and review the Data configuration file specified on the SYSFTPD DD statement in the FTP started
task JCL.

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

1. The SMF statement is coded with a value of STD.
2. The SMFJES and SMFSQL statements are coded without an additional value.
3. The SMFAPPE, SMFDEL, SMFEXIT, SMFLOGN, SMFREN,
SMFRETR, and SMFSTOR statements are not coded or commented out.

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

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

Fix Text: The system programmer will review the configuration statements in the
FTP.DATA data set and ensure the SMF options conform to the specifications in
the FTP.DATA Configuration Statements below or that they are commented out.

```
SMF       TYPE119
SMFJES       TYPE119
SMFSQL       TYPE119
SMFAPPE       [Not coded or commented out]
SMFDEL       [Not coded or commented out]
SMFEXIT       [Not coded or commented out]
SMFLOGN       [Not coded or commented out]
SMFREN       [Not coded or commented out]
SMFRETR       [Not coded or commented out]
SMFSTOR       [Not coded or commented out]
```

The FTP Server can provide audit data in the form of SMF records. SMF record
type 119, the TCP/IP Statistics record, can be written with the following subtypes:

70 Append
70 Delete and Multiple Delete
72 Invalid Logon Attempt
70 Rename
70 Get (Retrieve) and Multiple Get
70 Put (Store and Store Unique) and Multiple Put

SMF data produced by the FTP Server provides transaction information for both
successful and unsuccessful FTP commands. This data may provide valuable information for security audit activities. Type 119 records use a more standard
format and provide more information.

CCI: CCI-000130

CCI: CCI-000366

Group ID (Vulid): V-223734
Group Title: FT000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000020

Rule Title: The permission bits and user audit bits for HFS objects that are
part of the FTP Server component will be properly configured.

Vulnerability Discussion: HFS directories and files of the FTP Server provide
the configuration and executable properties of this product. Failure to properly
secure these objects may lead to unauthorized access resulting in the compromise
of the integrity and availability of the operating system environment, ACP, and
customer data.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
permission
bits and user audit bits for HFS objects that are part of the FTP Server component are
configured according to the settings in the FTP SERVER HFS OBJECT SECURITY
SETTINGS (4.4.4.2 a)

a) Using Vanguard Administrator UNIX file manager option 14 review the files
listed below.

b) If the HFS permission bits and user audit bits for each directory and file
match or
are more restrictive than the specified settings listed in the list below, there
is NO
FINDING.

HFS file name 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.
Absence of a file will not be considered a FINDING.

1. 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.

2. 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.

3. 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

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

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the 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-98177
Group Title: V-223735
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000030
Rule Title: MVS data sets for the FTP Server are not properly protected.

Vulnerability Discussion: MVS data sets of the FTP Server provide the configuration and operational characteristics of this product. Failure to properly secure these data sets may lead to unauthorized access resulting in the
compromise of the integrity and availability of customer data and some system
services.

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

Check Content:
The IAO will ensure that if present, the data set containing the FTP.DATA configuration
file allows read access to all authenticated users and all other access is
restricted to
systems programming personnel. The IAO will ensure that all write and allocate
access
to the data set containing the FTP.DATA configuration file is logged. The IAO

will
ensure that if present, the data set containing the FTP banner file allows read
access to all

a) Locate the SYSFTPD statement in all active FTPD started tasks JCL members
executing on the domain..

b) Using Vanguard Administrator Ensure the following data set controls are in
effect for the FTP Server:
1. Using On-line Access and Authorization option 4 review the profile protecting
the dataset identified in (A) UPDATE and ALTER access to the data set containing the FTP Data configuration file is restricted to systems programming personnel.
 Document the protecting profile(s)

 NOTE: READ access to all authenticated users is permitted.

2. Using AUDIT FLAGS option 3;3;2 review all profiles identified in (1) to
ensure UPDATE and ALTER access to the data set containing the FTP Data configuration file is logged.

3. From the ISPF Primary Option Menu use option 3.4 and review the banner statement located in the FTP configuration file. Using On-line Access and Authorization option 4 review the profile protecting the dataset identified to
ensure UPDATE and ALTER access to the data set containing the FTP banner file is restricted to systems programming personnel.

4. From the ISPF Primary Option Menu use option 3.4 and review the banner statement located in the FTP configuration file. Using AUDIT FLAGS option 3;3;2 review all profiles identified in (1) READ access to the data set containing the FTP banner file is permitted to all authenticated users.

NOTES:
The MVS data sets mentioned above are not used in every configuration. Absence of a data set will not be considered a FINDING.

The data set containing the FTP Data configuration file is determined by checking
the SYSFTPD DD statement in the FTP started task JCL.

The data set containing the FTP banner file is determined by checking the BANNER statement in the FTP Data configuration file.

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

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

Fix Text: Review the data set access authorizations defined to the ACP for the
FTP.DATA and FTP.BANNER files. Ensure these data sets are protected as follows:

The data set containing the FTP.DATA configuration file allows read access to
all authenticated users and all other access is restricted to systems programming personnel.

All write and allocate access to the data set containing the FTP.DATA configuration file is logged.

The data set containing the FTP banner file allows read access to all authenticated users and all other access is restricted to systems programming
personnel.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223736
Group Title: FT000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000040
Rule Title: IBM z/OS FTP.DATA configuration statements must have a proper BANNER
statement with the Standard Mandatory DoD Notice and Consent Banner.

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and
security notification verbiage used is consistent with applicable federal laws,
Executive Orders, directives, policies, regulations, standards, and guidance.
System use notifications are required only for access via logon interfaces with
human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the
following verbiage for operating systems that can accommodate banners of 1300
characters:

"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."

Use the following verbiage for operating systems that have severe limitations on
the number of characters that can be displayed in the banner:

"I've read consent to terms in IS user agreem't."

Responsibility: Systems Programmer
IAControls: SRG-OS-000023-GPOS-00006, SRG-OS-000024-

Check Content:

The systems programmer responsible for supporting ICS will ensure that for
systems at
Z/OS Release 2.10 and above, the FTP.DATA BANNER parameter specifies an HFS file
or Z/OS data set that contains the warning logon banner.

a) From the ISPF Primary Option Menu use option 3.4 and review the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

b) Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI
investigative searching or monitoring of the content of privileged communications, or
work product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product
are private and confidential. See User Agreement for details.

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

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

Fix Text:
Review the file specified by the FTP.DATA BANNER parameter. Ensure the text in
this file specifies a logon banner in accordance with DISA requirements.

Ensure the BANNER statement in the FTP Data configuration file specifies an HFS
file or z/OS data set that contains a logon banner. The below banner is
mandatory and deviations are not permitted except as authorized in writing by
the DoD Chief Information Officer. The thrust of this new policy is to make it
clear that there is no expectation of privacy when using DoD information systems
and all use of DoD information systems is subject to searching, auditing,
inspecting, seizing, and monitoring, even if some personal use of a system is
permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement (LE),
and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG authorized purpose.

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-223737
Group Title: FT000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000050
Rule Title: The warning banner for the FTP Server is not specified properely.

Vulnerability Discussion: System use notifications are required only for access
via logon interfaces with human users and are not required when such human
interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the
following verbiage for operating systems that can accommodate banners of 1300
characters:

"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."

Use the following verbiage for operating systems that have severe limitations on
the number of characters that can be displayed in the banner:

"I've read consent to terms in IS user agreem't."

Documentable: YES
Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:
The systems programmer responsible for supporting ICS will ensure that for
systems at
Z/OS Release 2.10 and above, the FTP.DATA BANNER parameter specifies an HFS file
or Z/OS data set that contains the warning logon banner.

a) From the ISPF Primary Option Menu use option 3.4 and review the Data
configuration file specified on the SYSFTPD DD statement in the FTP started
task JCL.

b) Ensure the BANNER statement in the FTP Data configuration file specifies an
HFS file or data set that contains a logon banner. The below banner is mandatory
and deviations are not permitted except as authorized in writing by the DoD
Chief
Information Officer. The thrust of this new policy is to make it clear that
there is

no expectation of privacy when using DoD information systems and all use of
DoD information systems is subject to searching, auditing, inspecting, seizing,
and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided
for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to
the
following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject
to routine
monitoring, interception, and search, and may be disclosed or used for any USG
authorized purpose.

-This IS includes security measures (e.g., authentication and access controls)
to protect
USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI
investigative searching or monitoring of the content of privileged communications, or
work product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product
are private and confidential. See User Agreement for details.

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

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

Fix Text: Review the file specified by the FTP.DATA BANNER parameter. Ensure the text in this file specifies a logon banner in accordance with DISA requirements.

Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or z/OS data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223739
Group Title: FT000070
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000070
Rule Title: FTP.DATA configuration statements for the FTP Server are not specified in accordance with requirements.

Vulnerability Discussion: The statements in the FTP.DATA configuration file specify the parameters and values that control the operation of the FTP Server components including the use of anonymous FTP. Several of the parameters must have specific settings to provide a secure configuration. Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the FTP Server FTP.DATA configuration statements are coded according to the settings in the OS390 STIG Volume 1 Table 4.4.41.3.a

FTP.DATA CONFIGURATION STATEMENTS
ANONYMOUS_ [Not Coded]
BANNER [An HFS file, e.g., /etc/ftp.banner]
INACTIVE_ [A value between 1 and 900]
UMASK_ 077

a) Display the active started tasks executing on the domain using SDSF, or

equivalent
JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate
the
FTP JCL member. NOTE: the JCL member is typically named FTPD.

b) Locate the SYSFTPD statement in all active FTPD started tasks JCL members
executing on the domain.

c) From the ISPF Primary Option Menu use option 3.4 and review the FTP daemon s
started task configuration identified by the SYSFTPD statement. Ensure the
following items are in effect for the configuration statements specified in the
FTP
Data configuration file:

1) The ANONYMOUS statement is not coded (does not exist) or, if it does exist,
it is commented out. _____ True _____ False

NOTE: Other statements prefixed with ANONYMOUS may be present. These statements
indicate the level of anonymous support and applicable restrictions if anonymous
support
is enabled using the ANONYMOUS statement. These other ANONYMOUS-prefixed
statements may be ignored.

2) The INACTIVE statement is coded with a value between 1 and 900 (seconds).
_____ True _____ False

NOTES: 900 indicates a session timeout value of 15 minutes.
 0 disables the inactivity timer check.

3) The UMASK statement is coded with a value of 077. ____ True ___ False

4) The BANNER statement is coded. _____ True _____ FALSE

d) If any items above are False this is a FINDING for STIG ID IPFTP030

Fix Text: Review the configuration statements in the FTP.DATA file and ensure
they conform to the specifications in the

FTP.DATA CONFIGURATION STATEMENTS below:

STATEMENT NOT CODED,

CODED WITHOUT VALUE,
OR PARAMETER VALUE

ANONYMOUS [Not Coded]

BANNER [An HFS file, e.g., /etc/ftp.banner]

INACTIVE [A value between 1 and 900]

UMASK 077 [See Note 1]

NOTE: If the FTP Server requires a UMASK value less restrictive than 077,
requirements should be justified and documented with the IAO.

CCI: CCI-000048

CCI: CCI-000366

CCI: CCI-001133

Group ID (Vulid): V-223740
Group Title: FT000080
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000080
Rule Title: The TFTP Server program is not properly protected.

Vulnerability Discussion: The Trivial File Transfer Protocol (TFTP) Server,
known as tftpd, supports file transfer according to the industry standard Trivial File Transfer Protocol. The TFTP Server does not perform any user identification or authentication, allowing any client to connect to the TFTP
Server. Due to this lack of security, the TFTP Server will not be used. Failure
to restrict the use of the TFTP Server may result in unauthorized access to the
host. This exposure may impact the integrity, availability, and privacy of
application data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
The IAO will ensure that Userid and password is coded on separate statements to
prevent
the display of the password in the output file.

a) Using Vanguard Administrator General Resource report option 3.4 Mask on
class=program

b) Ensure the following program controls are in effect for the TFTP Server:

1. Program resources TFTPD and EZATD are defined to the PROGRAM resource class with a UACC(NONE). The library name where these programs are located is hlq.TCPIP.SEZALOAD.

2. No access to the program resources TFTPD and EZATD is permitted.

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

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

Fix Text: Evaluate the impact of implementing the following change. Develop a
plan of action and implement the change as required.

1) Ensure that the EZATD program and its alias TFTPD are defined to RACF, no
access is granted, and WARN mode is not enabled. The following commands provide
a sample of how this can be accomplished.

```
rdef program tftpd addmem('sys1.tcpip.sezaload'//nopadchk) -
 data('Reference SRR PDI # IFTP0090') -
 audit(all(read)) uacc(none) owner(admin)

rdef program ezatd -
 addmem('sys1.tcpip.sezaload'//nopadchk) -
 data('Reference SRR PDI # IFTP0090') -
 audit(all(read)) uacc(none) owner(admin)
```

A PROGRAM class refresh will be necessary and can be accomplished with the
command:

```
setr when(program) refresh
```

CCI: CCI-001764

CCI: CCI-002235

Group ID (Vulid): V-223741
Group Title: FT000090
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000090

Rule Title: User exits for the FTP Server are in use without proper approval or
proper documentation.

Vulnerability Discussion: Several user exit points in the FTP Server component
are available to permit customization of its operating behavior. These exits can
be used to modify functions such as FTP command usage, client connection
controls, post processing tasks, and SMF record modifications. Without proper
review and adequate documentation of these exit programs, undesirable operations
and degraded security may result. This exposure could lead to unauthorized
access impacting data integrity or the availability of some system services, or
contribute to the loss of accountability and hamper security audit activities.

Responsibility: Information Assurance Manager
IAControls: DCCS-1, DCCS-2, DCSL-1, DCSW-1

Check Content:
The systems programmer responsible for supporting ICS will ensure that the FTP
Server
user exits are not implemented.

a) Refer to the Data configuration file specified on the SYSFTPD DD statement in
the FTP started task JCL. From the ISPF Primary Option Menu use option 3.4 and
review the file(s) allocated by the STEPLIB DD statement in the FTP started task
JCL.
1. Refer to the libraries specified in the system Linklist and LPA.
2. Refer to U_zOS_STIG_INSTRUCTION.doc for the information gathered from the IBM
Communications Server Worksheet in the Preliminary Information Worksheets.

b) Ensure the following items are in effect for FTP Server user exits:
The FTCHKCMD, FTCHKIP, FTCHKJES, FTCHKPWD, FTPSMFEX and FTPOSTPR modules are not
located in the FTP daemon s STEPLIB, Linklist, or LPA.
NOTE: The ISPF ISRFIND utility can be used to search the system Linklist and
LPA for specific modules.

Ensure that SMFEXIT= is not specified in the FTP DATA configuration file
enabling the FTPSMFEX exit.

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

d) If any FTP Server user exits are implemented and the site has written approval
from DISA FSO to install and use the exits, there is NO FINDING.

e) If any FTP Server user exits are implemented and the site has not obtained
written
approval from FSO to install and use the exits, this is a FINDING.

Fix Text: Review the configuration statements in the FTP.DATA file. Review the
FTP daemon STEPLIB, system Linklist, and Link Pack Area libraries. If FTP Server
exits are enabled or present, and have not been approved by the site IAM and not
securely written and implemented by the site systems programmer, they should not
be installed. Verify that non of the following exits are installed unless they
have met the requirements listed above:
FTCHKCMD
FTCHKIP
FTCHKJES
FTCHKPWD
FTPOSTPR
FTPSMFEX

CCI: CCI-000382

CCI: CCI-001764

CCI: CCI-001765

Group ID (Vulid): V-223742
Group Title: FT000100
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000100
Rule Title: The FTP Server daemon is not defined with proper security parameters.

Vulnerability Discussion: The FTP Server daemon requires special privileges and
access to sensitive resources to provide its system services. Failure to
properly define and control the FTP Server daemon could lead to unauthorized

access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:
The systems programmer responsible for supporting ICS will ensure that the FTP
daemon
runs under its own user account. Specifically, it does not share the account
defined for the
Z/OS UNIX kernel.

a) Display the active started tasks executing on the domain using SDSF, or
equivalent
JES display product, and locate the FTP daemon.
Find the FTPD USERID. Document the FTPD ID: _____

b) Display the active started tasks executing on the domain using SDSF, or
equivalent
JES display product, and locate the OMVS daemon.
Find the OMVS USERID. The OMVS USER ID is _____

c) Review Vanguard Analyzer RACF Started Procedures Table Analysis option 3; 4

d) There is an entry in the STARTED resources class for FTP daemons _____ True
____
False

e) All of FTPD(s) USERID are FTPD _____ True _____False

f) The FTPD(S) USERID is not the same as OMVS USERID ____ True _____ False

g) The FTPD(s) USERIDs are defined as a PROTECTED ____ True ____ False____

h) Review the FTP USERID with Vanguard Administrator User Reports option 3; 1
Mask on USERID=USERID documented above

1. Type LV on CMD space next to USER ID

2. Insure FTPD(s) userid has the following OMVS Segments attributes:
The UID value is 0 _____ True _____ False
There is a HOME directory / _____ True _____ False
There is a shell program defined /bin/sh _____ True _____ False

i) If any items above are False this is a FINDING for STIG ID IPFTP0010

Fix Text: Evaluate the impact of correcting any deficiencies. Develop a plan of
action and implement the required changes.
Ensure the following items are in effect for all MCS consoles:

1. The FTP daemon userid must be FTPD and a matching entry in the STARTED resource class exists enabling the use of the standard userid and an appropriate
group.

2. The FTPD userid is defined as a PROTECTED userid.

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

Sample commands to accomplish these requirements are shown here:

Add the FTPD userid:

```
AU FTPD NAME('STC, FTP Daemon') NOPASSWORD NOOIDCARD DFLTGRP(STCTCPX)
OWNER(STCTCPX) OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))

RDEF STARTED FTPD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
STDATA(USER(=MEMBER) GROUP(STCTCPX) TRACE(YES))
```

Additional permissions may be required. See SYS1.TCPIP.SEZAINST(EZARACF) or IBM
Comm Server: IP Config Guide.

CCI: CCI-000764

Group ID (Vulid): V-223744
Group Title: FT000120
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): FT000120
Rule Title: The startup parameters for the FTP include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords. The FTP daemon s started task JCL does not
specify the SYSTCPD and SYSFTPD DD statements for configuration files.

Vulnerability Discussion: During initialization, the FTP daemon reads JCL
keywords and configuration files to determine values for critical operational
parameters. Because system security is impacted by some of these parameter

settings, controlling these options through the configuration file only and
explicitly specifying the file locations reduces ambiguity, enhances security
auditing, and ensures proper operations. Inappropriate values could result in
undesirable operations and degraded security. This exposure may result in
unauthorized access impacting data integrity or the availability of some system
services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, IAIA-1, IAIA-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the
startup
parameters for the FTP daemon does not include the ANONYMOUS, ANONYMOUS=,
or INACTIVE keywords

a) Display the active started tasks executing on the domain using SDSF, or
equivalent
JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate
the FTP
JCL member. NOTE: The JCL member is typically named FTPD.

Display the active started tasks executing on the domain using SDSF, or
equivalent
JES display product, and locate the TCPIP started tasks.

b) Review the FTP daemon s started task JCL:

1. The SYSTCPD and SYSFTPD DD statements specify the TCP/IP Data and
FTP Data configuration files respectively. _____ True _____ False

2. The ANONYMOUS keyword is not coded on the PARM parameter on the
EXEC statement. _____ True _____ False

3. The ANONYMOUS=logonid combination is not coded on the PARM
parameter on the EXEC statement. _____ True _____ False

4. The INACTIVE keyword is not coded on the PARM parameter on the EXEC
statement. _____ True _____ FALSE

The AUTOLOG statement block can be configured to have TCP/IP start the
FTP
Server. The FTP entry (e.g., FTPD) can include the PARMSTRING parameter
to

pass parameters to the FTP procedure when started. NOTE: Parameters passed on
the PARMSTRING parameter override parameters specified in the FTP procedure

c) Review the AUTOLOG statement block with in the PROFILE DD of the each TCPIP started task JCL. If an FTP entry is configured in the AUTOLOG statement block in the TCP/IP Profile configuration file, ensure the following
items are in effect:

1. The ANONYMOUS keyword is not coded on the PARMSTRING parameter.

2. The ANONYMOUS=logonid combination is not coded on the PARMSTRING parameter.

3. The INACTIVE keyword is not coded on PARMSTRING parameter.

d) If any items above are False this is a FINDING for STIG ID IFTPP020

Fix Text: Review the FTP daemon s started task JCL. Ensure that the ANONYMOUS
and INACTIVE startup parameters are not specified and configuration file names
are specified on the appropriate DD statements.

The FTP daemon program can accept parameters in the JCL procedure that is used
to start the daemon. The ANONYMOUS and ANONYMOUS= keywords are designed to allow
anonymous FTP connections. The INACTIVE keyword is designed to set the timeout
value for inactive connections. Control of these options is recommended through
the configuration file statements rather than the startup parameters.

The systems programmer responsible for supporting ICS will ensure that the
startup parameters for the FTP daemon does not include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords.

During initialization the FTP daemon searches multiple locations for the TCPIP.DATA and FTP.DATA files according to fixed sequences. In the daemon s
started task JCL, Data Definition (DD) statements will be used to specify the
locations of the files. The SYSTCPD DD statement identifies the TCPIP.DATA file
and the SYSFTPD DD statement identifies the FTP.DATA file.

The systems programmer responsible for supporting ICS will ensure that the FTP
daemon s started task JCL specifies the SYSTCPD and SYSFTPD DD statements for
configuration files.

CCI: CCI-000366

Group ID (Vulid): V-255935
Group Title: SRG-OS-0000
Rule ID: SV-252886r822547_rul
Severity: CAT II
Rule Version (STIG-ID): IC000010
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be correctly specified.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) product
has the ability to use privileged functions and/or have access to sensitive
data. Failure to properly configure parameter values could potentially the
integrity of the base product which could result in compromising the operating
system or sensitive data.

Responsibility: Systems Programmer
IAControls: n/a

Check Content:

The systems programmer responsible for supporting CSF will ensure that the CSF
Started task
is configured correctly.

Refer to the CSFPRMxx member in the logical PARMLIB concatenation.

If the configuration parameters are specified as follows this is not a finding.

REASONCODES(ICSF)
COMPAT(NO)
SSM(YES)
CHECKAUTH(YES)
FIPSMODE(YES,FAIL(NO))
AUDITKEYLIFECKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFEPKDS (TOKEN(YES),LABEL(YES)).

AUDITKEYLIFETKDS (TOKENOBJ(YES),SESSIONOBJ(YES)).
AUDITKEYUSGCKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITKEYUSGPKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITPKCS11USG (TOKENOBJ(YES),SESSIONOBJ(YES),NOKEY(YES),INTERVAL(n)).

DEFAULTWRAP should not be specified.

Note: Other options may be site defined.

Fix Text:

Evaluate the impact associated with implementation of the control options.
Develop a plan of action to implement the control options for CSFPRMxx as specified below:

REASONCODES(ICSF)
COMPAT(NO)
SSM(YES)
CHECKAUTH(YES)
FIPSMODE(YES,FAIL(NO))
AUDITKEYLIFECKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFEPKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFETKDS (TOKENOBJ(YES),SESSIONOBJ(YES)).
AUDITKEYUSGCKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITKEYUSGPKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITPKCS11USG (TOKENOBJ(YES),SESSIONOBJ(YES),NOKEY(YES),INTERVAL(n)).

DEFAULTWRAP should not be specified

Note: Other options may be site defined.

CCI: CCI-000035

Group ID (Vulid): V-255936
Group Title: SRG-OS-0000
Rule ID: SV-252887r822550_rul
Severity: CAT II
Rule Version (STIG-ID): IC000020
Rule Title: IBM Integrated Crypto Service Facility (ICSF) install data sets are
not properly protected.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) product
has the ability to use privileged functions and/or have access to sensitive

data. Failure to properly restrict access to their data sets could result in
violating the integrity of the base product which could result in compromising
the operating system or sensitive data.

Responsibility: Information Assurance Officer
IAControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Check with your IOA or Systems Programming personnel and compile the
list of IBM Integrated Crypto Service Facility (ICSF) install data sets,
Likely:
1. SYS1.CSF.**
2. From the Administrator Main Menu choose Option 2 Security Server Commands
3. then choose Option: 3 Data Set
4. Type the resource names collected in option a.1 above into: Enter fully
qualified (without quotes) data set or profile name:
_____
5. Hit enter.
6. Enter Y for Display covering profile? Y
7. Verify that the UACC is NONE
8. Verify that Audit Successes and Failures specifies UPDATE or READ.
9. Tab down to Standard Access Permits and place an E next to it (hit
enter)and validate that UPDATE or higher access is limited to Systems
Programming personnel. Verify that READ access is limited to Systems Programming
Personnel and Auditors and any other users that have a valid requirement to
utilize these data sets.Press F3 to return to previous screen.
10. if CONDITIONAL ACCESS PERMITS: _ (E to edit data) has *data is
present* next to it, place an E next to it and validate that conditional access
permits of Update or higher are limited to Systems Programming Personnel as
well. Verify that READ access is limited to Systems Programming Personnel and
Auditors and any other users that have a valid requirement to utilize these data
sets. Press F3 to return to previous screen.
11. Repeat steps 2 through 10 for all datasets in option a.1

b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.

c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

Fix Text:
The IAO will ensure that update and allocate access to IBM Integrated Crypto
Service Facility (ICSF) install data sets is limited to System Programmers only,
and all update and allocate access is logged. Read access can be given to Auditors and any other users that have a valid requirement to utilize these data
sets.

The installing Systems Programmer will identify and document the product data
sets and categorize them according to who will have update and alter access and
if required that all update and allocate access is logged. He will identify if
any additional groups have update 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.

Data sets to be protected will be:
SYS1.CSF

The following commands are provided as a sample for implementing data set controls:

```
ad 'SYS1.CSF.**' uacc(none) owner(sys1) -
       audit(success(update) failures(read)) -
      data('Vendor DS Profile: icsf')
pe 'SYS1.CSF.**' id(syspaudt tstcaudt) acc(a)
pe 'SYS1.CSF.**' id(icsfusrs) acc(r)

ad 'sys1.csf.scsfmod0.**' owner(sys1)
 data('apf auth icsf ds') -
 audit(success(update) failures(read)) uacc(none)
pe 'sys1.csf.scsfmod0.**' id(syspaudt tstcaudt) acc(a)

setr generic(dataset) refresh
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-255939
Group Title: SRG-OS-000
Rule ID: SV-252888r822553_rul
Severity: CAT II
Rule Version (STIG-ID): IC000030

Rule Title: IBM Integrated Crypto Service Facility (ICSF) STC data sets are not
properly protected.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) STC
have the ability to use privileged functions and/or have access to sensitive
data. Failure to properly restrict access to their data sets could result in
violating the integrity of the base product which could result in compromising
the operating system or sensitive data.

Responsibility: Information Systems Security Officer
IAControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1,

Check Content:

a) Check with your ISSO or Systems Programming personnel and compile the
list of IBM Integrated Crypto Service Facility (ICSF) datasets referenced in the
CSFPARM DD statement of the ICSF started task(s) and/or batch job(s), the
entries for CKDSN and PKDSN specify the data sets. They are Likely:
1. SYS3.CSF.CKDS and SYS3.CSF.PKDS.
2. From the Administrator Main Menu choose Option 2 Security Server Commands
3. then choose Option: 3 Data Set
4. Type the resource names collected in option a.1 above into: Enter fully
qualified (without quotes) data set or profile name:
_____
5. Hit enter.
6. Enter Y for Display covering profile? Y
7. Verify that the UACC is NONE
8. Verify that Audit Successes and Failures specifies UPDATE or READ.
9. Tab down to Standard Access Permits and place an E next to it (hit
enter) and validate that UPDATE or higher access is limited to Systems
Programming personnel, ICSF STC and/or batch jobs only. Verify that READ access
is limited to Auditors. Press F3 to return to previous screen.
10. if CONDITIONAL ACCESS PERMITS: _ (E to edit data) has *data is
present* next to it, place an E next to it and validate that conditional access
permits of UPDATE or higher access is limited to Systems Programming personnel,
ICSF STC and/or batch jobs only. Verify that READ access is limited to Auditors.
Press F3 to return to previous screen.

11. Repeat steps 2 through 10 for all datasets in option a.1

b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.

c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

Fix Text:
The ISSO will ensure that update and alter access to IBM Integrated Crypto Service Facility (ICSF) STC and/or batch data sets are limited to system programmers and ICSF STC and/or batch jobs only. Read access may be granted to auditors at the ISSOs discretion.

The installing systems programmer will identify and document the product data sets and categorize them according to who will have what type of access and if required what type of access is logged. He will identify if any additional groups requiring access to specific data sets, and once documented he will work with the ISSO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

The data sets to be protected are identified in the dataset referenced in the CSFPARM DD statement of the ICSF started task(s) and/or batch job(s), the entries for CKDSN and PKDSN specify the data sets.

Note: Currently on most CSD systems the CKDSN specifies SYS3.CSF.CKDS and PKDSN specifies SYS3.CSF.PKDS.

The following commands are provided as a sample for implementing dataset controls:

```
ad 'sys3.csf.**' uacc(none) owner(sys3) -
       audit(failures(read)) -
      data('ICSF Output Data')
pe 'sys3.csf.**' id(syspaudt) acc(a)
pe 'sys3.csf.**' id(tstcaudt) acc(a)
pe 'sys3.csf.**' id(icsfstc) acc(a)
pe 'sys3.csf.**' id(audtaudt) acc(r)
```

CCI: CCI-001499

Group ID (Vulid): V-255937
Group Title: SRG-OS-0001
Rule ID: SV-252889r822556_rul

Severity: CAT II
Rule Version (STIG-ID): IC000040
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started Task name is
not properly identified / defined to the system ACP.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) requires a started task that will be restricted to certain resources, datasets
and other system functions. By defining the started task as a userid to the
system ACP, It allows the ACP to control the access and authorized users that
require these capabilities. Failure to properly control these capabilities,
could compromise of the operating system environment, ACP, and customer data.

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

Check Content:

1. From the Vanguard Security Solutions choose Administrator Option 1.
2. choose 3 Security Server Reports
3. choose option 1 User Profiles. Make sure you are in Live mode by typing LIVE
on command line.
4. Tab down to USERID and type in CSFSTART. (CSFSTART is the userid that must be
associated with the started task profile.)
5. choose option 1, User Summary and hit enter.
6. If the report displays NO USERIDS TO REPORT, this is a finding.
7. If the report displays the User CSFSTART, place a UA next to the userid. If
the display does not show PT under the PROT column or shows No USERIDS to Report, then there is a Finding.
8. If the USERID exists and PT is specified in the PROT column, then there is no
finding.

Fix Text:
The Systems Programmer and IAO will ensure that the started task for IBM Integrated Crypto Service Facility (ICSF) Started Task(s) is properly Identified
/ defined to the System ACP.

If the product requires a Started Task, verify that it is properly defined to
the System ACP with the proper attributes.

Most installation manuals will indicate how the Started Task is identified and
any additional attributes that must be specified. Define the started task userid
CSFSTART for IBM Integrated Crypto Service Facility (ICSF).

Example:

```
AU CSFSTART NAME('STC, ICSF') NOPASS -
       OWNER(STC) DFLTGRP(STC) -
      DATA('START ICSF')
```

CCI: CCI-000764

Group ID (Vulid): V-255938
Group Title: SRG-OS-0000
Rule ID: SV-223653r604139_rul
Severity: CAT II
Rule Version (STIG-ID): IC000050
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started Task name is
not properly identified / defined to the system ACP.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) requires a started task that will be restricted to certain resources, datasets
and other system functions. By defining the started task as a userid to the
system ACP, It allows the ACP to control the access and authorized users that
require these capabilities. Failure to properly control these capabilities,
could compromise of the operating system environment, ACP, and customer data.

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

Check Content:

1. From the Vanguard Security Solutions choose Administrator Option 1.
2. choose 3 Security Server Reports
3. choose option 1 User Profiles. Make sure you are in Live mode by typing LIVE
on command line.

4. Tab down to USERID and type in CSFSTART. (CSFSTART is the userid that must be
associated with the started task profile.)
5. choose option 1, User Summary and hit enter.
6. If the report displays NO USERIDS TO REPORT, this is a finding.
7. If the report displays the User CSFSTART, place a UA next to the userid. If
the display does not show PT under the PROT column or shows No USERIDS to Report, then there is a Finding.
8. If the USERID exists and PT is specified in the PROT column, then there is no
finding.

Fix Text:
The Systems Programmer and IAO will ensure that the started task for IBM Integrated Crypto Service Facility (ICSF) Started Task(s) is properly Identified
/ defined to the System ACP.

If the product requires a Started Task, verify that it is properly defined to
the System ACP with the proper attributes.

Most installation manuals will indicate how the Started Task is identified and
any additional attributes that must be specified. Define the started task userid
CSFSTART for IBM Integrated Crypto Service Facility (ICSF).

Example:

```
AU CSFSTART NAME('STC, ICSF') NOPASS -
       OWNER(STC) DFLTGRP(STC) -
      DATA('START ICSF')
```

CCI: CCI-000764

Group ID (Vulid): V-223745
Group Title: JS000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000010
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.

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

Check Content:
a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB
member used to start JES2.
b) Review the NJE definitions by searching for NODE (in the member). Note the
NAME= parameter for each occurrence.
c) Review the workstation definitions by searching for RMT (in the member).
d) From Administrator Main Menu, select option 3 Security Server Reports; press
ENTER.
e) Choose Option 4 General Resource Profile; press Enter.
f) choose Option1 General Resource Profile Summary; type FACILITY next to class
under Standard Masking Fields. Press ENTER.
g) Review the following resource definitions in the FACILITY 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

NOTE 2: Workstation is RMTnnnn, where nnnn is the number on the RMT statement.
Review the JES2 parameters for RJE workstation definitions

h) If all JES2 defined NJE nodes and RJE workstations have a profile defined in
the FACILITY resource class, there is NO FINDING
i) If any JES2 defined NJE node or RJE workstation does not have a profile
defined in the FACILITY resource 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-223746
Group Title: JS000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000020
Rule Title: JES2 input sources are not controlled in accordance with theh proper
security requirements.

Vulnerability Discussion: JES2 input sources provide a variety of channels for
job submission. Failure to properly control the use of these input sources could
result in unauthorized submission of work into the operating system. This exposure may threaten the integrity and availability of the operating system
environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.

b) Review the spool offload receiver definitions by searching for OFF(in the
member.

c) Review the local card reader definitions by searching for RDR(in the member.

d) Use the list of RJE workstations from ZJES0011 and the list of NJE nodes from
ZJES012.

e) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

f) Select option 4 General Resource Profile

g) On the General Resources Reports panel, enter INTRDR in the Profile field,

enter
JESINPUT in the Class field and enter B for Batch/Online. Press ENTER

h) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

i) Save the output for use in the INTRDR (internal reader for batch jobs) check.

j) Using the node list mentioned in step d, on the General Resources Reports
panel,
enter nodename in the Profile field, enter JESINPUT in the Class field and enter
B for Batch/Online. Press ENTER

k) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

l) Save the output for use in the nodename (NJE node) check.

m) Repeat step j through l for each nodename in the list

n) On the General Resources Reports panel, enter OFF* in the Profile field,
enter
JESINPUT in the Class field and enter B for Batch/Online. Press ENTER

o) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

p) Save the output for use in the OFFn.* (spool offload receiver) check.

q) On the General Resources Reports panel, enter R%%%%.* in the Profile field,
enter JESINPUT in the Class field and enter B for Batch/Online. Press
ENTER

r) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

s) Save the output for use in the Rnnnn (RJE workstation) check.

t) On the General Resources Reports panel, enter RDR.* in the Profile field,
enter
JESINPUT in the Class field and enter B for Batch/Online. Press ENTER

u) On the JCL Submit Processing panel, enter S on the command line to submit the

job. Press ENTER

v) Save the output for use in the RDRnn (local card reader) check.

w) On the General Resources Reports panel, enter STCINRDR in the Profile field,
enter JESINPUT in the Class field and enter B for Batch/Online. Press ENTER

x) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

y) Save the output for use in the STCINRDR (internal reader for started tasks
jobs)
check.

z) On the General Resources Reports panel, enter TSUINRDR in the Profile field,
enter JESINPUT in the Class field and enter B for Batch/Online. Press ENTER

aa) On the JCL Submit Processing panel, enter S on the command line to submit
the
job. Press ENTER

bb) Save the output for use in the TSUINRDR (internal reader for TSO logons)
check.

cc) From Administrator main Menu, select option 2 Security Server Commands.
Press ENTER

dd) From the VRC main menu, select option 5 SETROPTS. Press ENTER

ee) Under Class Options, enter E after CDT Classes. Press ENTER

ff) Enter L JESINPUT on the command line. Note if there is a Y under the column
labeled ACT. If yes, this indicates the class is active. Print the screen and
save it
for the class active check.

gg) Review the following resources in the JESINPUT resource class:
* INTRDR (internal reader for batch jobs) review output from step i.
* nodename (NJE node) review output from step l.
* OFFn.* (spool offload receiver) review output from step p.
* Rnnnn (RJE workstation) review output from step s.
* RDRnn (local card reader) review output from step v.
* STCINRDR (internal reader for started tasks) review output from step y.

* TSUINRDR (internal reader for TSO logons) review output from step bb.
NOTE: If any of these are not found, that resource in the JESINPUT resource
class does not have to be defined.

hh) Ensure the following items are in effect:
1. The JESINPUT resource class is active (obtained in step ff).
2. The resources mentioned in step gg are protected by generic and/or fully
qualified profiles defined to the JESINPUT resource class.
3. UACC(NONE) is specified for all resources.
4. NOTE: UACC(READ) is allowed for input sources that are permitted to
submit jobs for all users. Currently, the Z/OS STIG provides no guidance on
which input sources are appropriate for UACC(READ). However, common
sense should prevail during the analysis. For example, UACC(READ) would
typically be inappropriate for RJE, NJE, offload, and STC input sources.

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

jj) If any of the items mentioned in (hh) is untrue, this is a FINDING.

Fix Text: Review the following resources in the JESINPUT resource class:

INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.* (spool offload receiver)
Rnnnn (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

NOTE: If any of the following are not defined within the JES2 parameters, the
resource in the JESINPUT resource class does not have to be defined.

NOTE 1: Nodename is the NAME parameter in the NODE statement. Review the JES2
parameters for NJE node definitions by searching for NODE(in the report.

NOTE 2: OFFn, where n is the number of the offload receiver. Review the JES2
parameters for spool offload receiver definitions by searching for OFF(in the
report.

NOTE 3: Rnnnn, where nnnn is the number of the remote workstation. Review the
JES2 parameters for RJE node definitions by searching for RMT(in the
report.

NOTE 4: RDRnn, where nn is the number of the reader. Review the JES2
parameters

for reader definitions by searching for RDR(in the report.

c) Ensure the following items are in effect:

1) The JESINPUT resource class is active.

2) The resources mentioned in (b) are protected by generic and/or fully qualified profiles defined to the JESINPUT resource class.

3) UACC(NONE) is specified for all resources.

NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs
for all users. Currently, there is no guidance on which input sources are appropriate for UACC(READ). However, common sense should prevail during the
analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE,
offload, and STC input sources.

Examples:

```
setr classact(jesinput)
setr generic(jesinput)
rdef jesinput intrdr uacc(none) owner(admin) audit(failures(read)
success(update)) data('Per SRR PDI ZJES0021')
pe intrdr cl(jesinput) id(<syspaudt>)
pe intrdr cl(jesinput) id(*) /* all users */
```

CCI: CCI-000213

CCI: CCI-001310

Group ID (Vulid): V-223747
Group Title: JS000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000030
Rule Title: JES2 input sources must be properly controlled.

Vulnerability Discussion: JES2 input sources provide a variety of channels for
job submission. Failure to properly control the use of these input sources could
result in unauthorized submission of work into the operating system. This exposure may threaten the integrity and availability of the operating system
environment, and compromise the confidentiality of customer data.

Responsibility: N/A
IAControls: N/A

Check Content:
a) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

b) Select option 4 General Resource Profile

c) On the General Resources Reports panel, enter JESINPUT in the Class field and
enter B for Batch/Online. Select option 4 Access Lists and press ENTER

d) On the Processing Options Panel, enter Y for Explode RACF groups in access
list at end of report? and Explode Users/Groups in Surrogate ID access list at
end of report? Press ENTER

e) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

f) Review the output to determine access authorization for resources defined to
the
JESINPUT resource class.

g) If access authorization for resources defined to the JESINPUT resource class
is
restricted to the appropriate personnel, there is NO FINDING.

h) 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).If access authorization for any resource defined to the JESINPUT resource
class is inappropriate, this is a FINDING.

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-223748
Group Title: JS000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000040
Rule Title: JES2 output devices are not controlled in accordance with the proper
security requirements.

Vulnerability Discussion: JES2 output devices provide a variety of channels to
which output can be processed. Failure to properly control these output devices
could result in unauthorized personnel accessing output. This exposure may
compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Determine the JES2PARM member as specified in the HASPPARM DD of the
PROCLIB member used to start JES2.

b) Review the local printer definitions by searching for PRT(or PRINTER in the
member.

c) Review the local card definitions by searching for PUN(or PUNCH in the
member.

d) Review the remote workstation printer definitions by searching for .PR in the
member.

e) Review the remote workstation punch definitions by searching for .PU in the

member.

f) Use the list of NJE nodes from ZJES012 and the list of offload receivers from
ZJES0021.

g) From Administrator main Menu, select option 9 Analyzer. Press ENTER

h) From Analyzer main menu, select 4 Batch Reports. Press ENTER

i) From Batch Reports menu, select F Subsystem Name Table Analysis. Press ENTER

j) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press ENTER

k) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press ENTER

l) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

m) Review the output. Note that the first entry in the report is the JES2 subsystem
name and is typically JES2. This will be used in step p.

n) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

o) Select option 4 General Resource Profile

p) In all profile names, replace JES2 with the JES2 subsystem name determined in
step m.

q) On the General Resources Reports panel, enter JES2.** in the Profile field,
enter
WRITER in the Class field and enter B for Batch/Online. Press ENTER

r) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

s) Save the output for use in the JES2.** (backstop profile) check.

t) On the General Resources Reports panel, enter JES2.LOCAL.OFF%.* in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

u) On the JCL Submit Processing panel, enter S on the command line to submit the

job. Press ENTER

v) Save the output for use in the JES2.LOCAL.OFFn.*, JES2.LOCAL.OFFn.ST, and JES2.LOCAL.OFFn.JT (spool offload related) checks.

w) On the General Resources Reports panel, enter JES2.LOCAL.PRT% in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

x) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

y) Save the output for use in the JES2.LOCAL.PRTn ((local printer)) checks.

z) On the General Resources Reports panel, enter JES2.LOCAL.PUN% in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

aa) On the JCL Submit Processing panel, enter S on the command line to submit
the
job. Press ENTER

bb) Save the output for use in the JES2.LOCAL.PUNn (local punch) check.

cc) Using the node list mentioned in step f, on the General Resources Reports
panel,
enter nodename in the Profile field, enter JESINPUT in the Class field and enter
B for Batch/Online. Press ENTER

dd) On the JCL Submit Processing panel, enter S on the command line to submit
the
job. Press ENTER

ee) Save the output for use in the nodename (NJE node) check.

ff) Repeat step u through w for each nodename in the list

gg) On the General Resources Reports panel, enter JES2.RJE.R%%%%.P* in the
Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

hh) On the JCL Submit Processing panel, enter S on the command line to submit
the

job. Press ENTER

ii) Save the output for use in the JES2.RJE.Rnnnn.PRm and JES2.RJE.Rnnnn.PUm
(remote printer and punch) checks.

jj) From Administrator main Menu, select option 2 Security Server Commands.
Press ENTER

kk) From the VRC main menu, select option 5 SETROPTS. Press ENTER

ll) Under Class Options, enter E after CDT Classes. Press ENTER

mm) Enter L WRITER on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen
and save it for the class active check.

nn) Review the following resources in the WRITER resource class where JES2 is
the
name of the JES2 subsystem:
* JES2.** (backstop profile) review output from step s.
* JES2.LOCAL.OFFn.* (spool offload transmitter) review output from step v.
* JES2.LOCAL.OFFn.ST (spool offload SYSOUT transmitter) review output from step v.
* JES2.LOCAL.OFFn.JT (spool offload job transmitter) review output from step v.
* JES2.LOCAL.PRTn (local printer) review output from step q.
* JES2.LOCAL.PUNn (local punch) review output from step t.
* JES2.NJE.nodename (NJE node) review output from step ee.
* JES2.RJE.Rnnnn.PRm (remote printer) review output from step ii.
* JES2.RJE.Rnnnn.PUm (remote punch) review output from step ii.
NOTE: If any of these are not found, that resource in the WRITER resource class
does not have to be defined.

oo) Ensure the following items are in effect:
5. The WRITER resource class is active (obtained in step mm).
6. The resources mentioned in step nn are protected by generic and/or fully
qualified profiles defined to the WRITER resource class.
7. UACC(NONE) is specified for all resources.
8. NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs for all users. Currently, the Z/OS STIG provides no guidance on
which input sources are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, offload, and STC input sources.

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

qq) If any of the items mentioned in (oo) is untrue, this is a FINDING.

Fix Text: WRITER Resource Definitions

Review the following resources in the WRITER resource class:

```
JES2.**                                (backstop profile)
JES2.LOCAL.OFFn.*             (spool offload transmitter)
JES2.LOCAL.OFFn.ST             (spool offload SYSOUT transmitter)
JES2.LOCAL.OFFn.JT             (spool offload job transmitter)
JES2.LOCAL.PRTn                   (local printer)
JES2.LOCAL.PUNn                   (local punch)
JES2.NJE.nodename                   (NJE node)
JES2.RJE.Rnnnn.PRm             (remote printer)
JES2.RJE.Rnnnn.PUm             (remote punch)
```

NOTE 1: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

NOTE 2: OFFn, where n is the number of the offload transmitter. Determine the numbers by searching for OFF(in the JES2 parameters.

NOTE 3: PRTn, where n is the number of the local printer. Determine the numbers by searching for PRT(in the JES2 parameters.

NOTE 4: PUNn, where n is the number of the local card punch. Determine the numbers by searching for PUN(in the JES2 parameters.

NOTE 5: Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report.

NOTE 6: Rnnnn.PRm, where nnnn is the number of the remote workstation and m is the number of the printer. Determine the numbers by searching for .PR in the JES2 parameters.

NOTE 7: Rnnnn.PUm, where nnnn is the number of the remote workstation and m is the number of the punch. Determine the numbers by searching for .PU in the JES2 parameters.

c) Ensure the following items are in effect:

1) The WRITER resource class is active.

2) The profile JES2.** is defined to the WRITER resource class with a UACC(NONE).

3) The other resources mentioned in (b) are protected by generic and/or fully qualified profiles defined to the WRITER resource class with UACC(NONE).

NOTE: UACC(READ) is allowed for output destinations that are permitted to route output for all users. Currently, there is no guidance on which output destinations are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, and offload output destinations.

Examples:

```
setr classact(writer)
setr gencmd(writer) generic(writer)
setr raclist(writer)
RDEF WRITER JES2.** owner(admin) AUDIT(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.** owner(admin) AUDIT(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.JT owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.ST owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PRT* owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PUN* owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.NJE.** owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.RJE.** owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')

pe JES2.** cl(writer) id(<syspaudt>)
pe JES2.LOCAL.** cl(writer) id(<syspaudt>)
pe JES2.LOCAL.OFF*.JT cl(writer) id(<syspaudt>)
pe JES2.LOCAL.OFF*.ST cl(writer) id(<syspaudt>)
pe JES2.LOCAL.PRT* cl(writer) id(<syspaudt>)
pe JES2.LOCAL.PUN* cl(writer) id(<syspaudt>)
pe JES2.NJE.** cl(writer) id(<syspaudt>)
pe JES2.RJE.** cl(writer) id(<syspaudt>)
setr racl(writer) Ref
```

CCI: CCI-000213

Group ID (Vulid): V-223749
Group Title: JS000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000050
Rule Title: IBM z/OS JES2 output devices must be properly controlled for classified systems.

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:

a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.

b) Review the local printer definitions by searching for PRT(or PRINTER in the member.

c) Review the local card definitions by searching for PUN(or PUNCH in the
member.

d) Review the remote workstation printer definitions by searching for .PR in the
member.

e) Review the remote workstation punch definitions by searching for .PU in the
member.

f) Use the list of NJE nodes from ZJES012 and the list of offload receivers from
ZJES0021.

g) From Administrator main Menu, select option 9 Analyzer. Press ENTER

h) From Analyzer main menu, select 4 Batch Reports. Press ENTER

i) From Batch Reports menu, select F Subsystem Name Table Analysis. Press ENTER

j) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press ENTER

k) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press ENTER

l) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

m) Review the output. Note that the first entry in the report is the JES2 subsystem
name and is typically JES2. This will be used in step p.

n) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

o) Select option 4 General Resource Profile

p) In all profile names, replace JES2 with the JES2 subsystem name determined in
step m.

q) On the General Resources Reports panel, enter JES2.** in the Profile field,
enter
WRITER in the Class field and enter B for Batch/Online. Press ENTER

r) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

s) Save the output for use in the JES2.** (backstop profile) check.

t) On the General Resources Reports panel, enter JES2.LOCAL.OFF%.* in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

u) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

v) Save the output for use in the JES2.LOCAL.OFFn.*, JES2.LOCAL.OFFn.ST, and JES2.LOCAL.OFFn.JT (spool offload related) checks.

w) On the General Resources Reports panel, enter JES2.LOCAL.PRT% in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

x) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

y) Save the output for use in the JES2.LOCAL.PRTn ((local printer)) checks.

z) On the General Resources Reports panel, enter JES2.LOCAL.PUN% in the Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

aa) On the JCL Submit Processing panel, enter S on the command line to submit
the
job. Press ENTER

bb) Save the output for use in the JES2.LOCAL.PUNn (local punch) check.

cc) Using the node list mentioned in step f, on the General Resources Reports
panel,
enter nodename in the Profile field, enter JESINPUT in the Class field and enter
B for Batch/Online. Press ENTER

dd) On the JCL Submit Processing panel, enter S on the command line to submit
the
job. Press ENTER

ee) Save the output for use in the nodename (NJE node) check.

ff) Repeat step u through w for each nodename in the list

gg) On the General Resources Reports panel, enter JES2.RJE.R%%%%.P* in the
Profile field, enter WRITER in the Class field and enter B for Batch/Online.
Press ENTER

hh) On the JCL Submit Processing panel, enter S on the command line to submit
the
job. Press ENTER

ii) Save the output for use in the JES2.RJE.Rnnnn.PRm and JES2.RJE.Rnnnn.PUm
(remote printer and punch) checks.

jj) From Administrator main Menu, select option 2 Security Server Commands.
Press ENTER

kk) From the VRC main menu, select option 5 SETROPTS. Press ENTER

ll) Under Class Options, enter E after CDT Classes. Press ENTER

mm) Enter L WRITER on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen
and save it for the class active check.

nn) Review the following resources in the WRITER resource class where JES2 is
the
name of the JES2 subsystem:
* JES2.** (backstop profile) review output from step s.
* JES2.LOCAL.OFFn.* (spool offload transmitter) review output from step v.
* JES2.LOCAL.OFFn.ST (spool offload SYSOUT transmitter) review output from step v.
* JES2.LOCAL.OFFn.JT (spool offload job transmitter) review output from step v.
* JES2.LOCAL.PRTn (local printer) review output from step q.
* JES2.LOCAL.PUNn (local punch) review output from step t.
* JES2.NJE.nodename (NJE node) review output from step ee.
* JES2.RJE.Rnnnn.PRm (remote printer) review output from step ii.
* JES2.RJE.Rnnnn.PUm (remote punch) review output from step ii.
NOTE: If any of these are not found, that resource in the WRITER resource class
does not have to be defined.

oo) Ensure the following items are in effect:
5. The WRITER resource class is active (obtained in step mm).
6. The resources mentioned in step nn are protected by generic and/or fully
qualified profiles defined to the WRITER resource class.

7. UACC(NONE) is specified for all resources.
8. NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs for all users. Currently, the Z/OS STIG provides no guidance on
which input sources are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, offload, and STC input sources.

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

qq) If any of the items mentioned in (oo) is untrue, this is a FINDING.

Fix Text:
WRITER Resource Definitions

Review the following resources in the WRITER resource class:

```
JES2.**                                (backstop profile)
JES2.LOCAL.OFFn.*             (spool offload transmitter)
JES2.LOCAL.OFFn.ST             (spool offload SYSOUT transmitter)
JES2.LOCAL.OFFn.JT             (spool offload job transmitter)
JES2.LOCAL.PRTn                   (local printer)
JES2.LOCAL.PUNn                   (local punch)
JES2.NJE.nodename                   (NJE node)
JES2.RJE.Rnnnn.PRm             (remote printer)
JES2.RJE.Rnnnn.PUm             (remote punch)
```

NOTE 1: JES2 is typically the name of the JES2 subsystem. Refer to the
SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY
SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

NOTE 2: OFFn, where n is the number of the offload transmitter. Determine
the numbers by searching for OFF(in the JES2 parameters.

NOTE 3: PRTn, where n is the number of the local printer. Determine the
numbers by searching for PRT(in the JES2 parameters.

NOTE 4: PUNn, where n is the number of the local card punch. Determine the
numbers by searching for PUN(in the JES2 parameters.

NOTE 5: Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for
NODE(in the report.

NOTE 6: Rnnnn.PRm, where nnnn is the number of the remote workstation and

m is the number of the printer. Determine the numbers by searching for .PR in
the JES2 parameters.

NOTE 7: Rnnnn.PUm, where nnnn is the number of the remote workstation and
m is the number of the punch. Determine the numbers by searching for .PU in the
JES2 parameters.

c) Ensure the following items are in effect:

1) The WRITER resource class is active.

2) The profile JES2.** is defined to the WRITER resource class with a
UACC(NONE).

3) The other resources mentioned in (b) are protected by generic and/or
fully qualified profiles defined to the WRITER resource class with
UACC(NONE).

NOTE: UACC(READ) is allowed for output destinations that are permitted to
route output for all users. Currently, there is no guidance on which output
destinations are appropriate for UACC(READ). However, common sense should
prevail during the analysis. For example, UACC(READ) would typically be
inappropriate for RJE, NJE, and offload output destinations.

Examples:

```
setr classact(writer)
setr gencmd(writer) generic(writer)
setr raclist(writer)
RDEF WRITER JES2.** owner(admin) AUDIT(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.** owner(admin) AUDIT(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.JT owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.ST owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PRT* owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PUN* owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.NJE.** owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.RJE.** owner(admin) audit(ALL) UACC(NONE) -
 data('Reference SRR PDI ZJES0031')

pe JES2.** cl(writer) id(<syspaudt>)
```

```
pe JES2.LOCAL.** cl(writer) id(<syspaudt>)
pe JES2.LOCAL.OFF*.JT cl(writer) id(<syspaudt>)
pe JES2.LOCAL.OFF*.ST cl(writer) id(<syspaudt>)
pe JES2.LOCAL.PRT* cl(writer) id(<syspaudt>)
pe JES2.LOCAL.PUN* cl(writer) id(<syspaudt>)
pe JES2.NJE.** cl(writer) id(<syspaudt>)
pe JES2.RJE.** cl(writer) id(<syspaudt>)
setr racl(writer) Ref
```

CCI: CCI-000000

Group ID (Vulid): V-223750
Group Title: JS000060
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000060
Rule Title: JESSPOOL resources are not protected in accordance with security requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG, JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing userid and password information. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) From Administrator main Menu, select option 2 Security Server Commands.
Press ENTER

b) From the VRC main menu, select option 5 SETROPTS. Press ENTER

c) Under Class Options, enter E after CDT Classes. Press ENTER

d) Enter L JESSPOOL on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen and save it for the class active check.

e) Ensure that the JESSPOOL resource class is active (obtained in step d).

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

g) If any of the items mentioned in (e) is untrue, this is a FINDING.

Fix Text: Ensure that the JESSPOOL resource class is active:

Use the RACF Command: SETROPTS CLASSACT(JESSPOOL).

Note that you should also enable GENERICS and optionally RACLIST this class in
memory.

SETR GENERIC(JESSPOOL) GENCMD(JESSPOOL)
SETR RACLIST(JESSPOOL)

CCI: CCI-000213

Group ID (Vulid): V-223751
Group Title: JS000070
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000070
Rule Title: JESNEWS rewsources are not protected in accordance with security
requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG,
JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system
activity logs, and trace data containing userid and password information. This
exposure may threaten the integrity and availability of the operating system
environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.

b) From Administrator main Menu, select option 9 Analyzer. Press ENTER

c) From Analyzer main menu, select 4 Batch Reports. Press ENTER

d) From Batch Reports menu, select F Subsystem Name Table Analysis. Press <ENTER>

e) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press ENTER

f) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press ENTER

g) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press ENTER

h) Review the output. Note that the first entry in the report is the JES2 subsystem name and is typically JES2. This will be used in step k.

i) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>

j) Select option 4 General Resource Profile

k) In all profile names, replace JES2 with the JES2 subsystem name determined in step h.

l) On the General Resources Reports panel, enter JES2.UPDATE.JESNEWS in the Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online. Enter 2 on the command line to select Audit Flags and Press ENTER

m) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press ENTER

n) Save the output for use in the JES2.UPDATE.JESNEWS audit checks.

o) On the General Resources Reports panel, enter JESINPUT in the Class field and enter B for Batch/Online. Select option 4 Access Lists and Press ENTER

p) On the Processing Options Panel, enter Y for Explode RACF groups in access list at end of report? and Explode Users/Groups in Surrogate ID access list at end of report? Press ENTER

q) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press ENTER

r) Save the output for use in the JES2.UPDATE.JESNEWS audit checks.

s) On the General Resources Reports panel, enter JES2.UPDATE.JESNEWS in the
Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online.
Press ENTER

t) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

u) Save the output for use in the JES2.UPDATE.JESNEWS UACC checks.

v) Ensure the following items are in effect:

1. The JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource class with a default access of NONE and all access is logged.

2. Access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.

w) If both of the items in (v) are true, there is NO FINDING.

x) If either item in (v) is untrue, this is a FINDING.

Fix Text: JESNEWS Access Controls

Refer to "Protecting JESNEWS" in Chapter 7 of the JES2 Init & Tuning Guide.

a) Ensure the following items are in effect:

1) The JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource
class with a default access of NONE and all access is logged.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the
SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY
SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

2) Access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts CONTROL access to the appropriate personnel (i.e.,
users responsible for maintaining the JES News data set) and all access is
logged.

Examples of setting up proper protection are shown here:

```
RDEF OPERCMDS JES2.UPDATE.JESNEWS UACC(NONE) OWNER(ADMIN)
AUDIT(ALL(READ))
DATA('COMPLY WITH ZJES0042')

PERMIT JES2.UPDATE.JESNEWS CLASS(OPERCMDS) ID(<syspaudt>) ACCESS(CONTROL)
```

CCI: CCI-000213

CCI: CCI-001762

CCI: CCI-002234

Group ID (Vulid): V-223752
Group Title: JS000080
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000080
Rule Title: JESTRACE and/or SYSLOG resources are not protected in accordance
with security requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG,
JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system
activity logs, and trace data containing userid and password information. This
exposure may threaten the integrity and availability of the operating system
environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Use the list of NJE nodes from ZJES012 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.

b) From Administrator main Menu, select option 9 Analyzer. Press ENTER

c) From Analyzer main menu, select 4 Batch Reports. Press ENTER

d) From Batch Reports menu, select F Subsystem Name Table Analysis. Press ENTER

e) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press ENTER

f) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press ENTER

g) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

h) Review the output. Note that the first entry in the report is the JES2 subsystem
name and is typically JES2. This will be used in step k.

i) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

j) Select option 4 General Resource Profile

k) In all profile names, replace localnodeid with the NAME parameter from the
node determined as OWNNODE in step a and replace JES2 with the JES2 subsystem name determined in step h.

l) On the General Resources Reports panel, enter localnodeid.JES2.* in the
Profile
field, enter JESSPOOL in the Class field and enter B for Batch/Online. Select
option 4 Access Lists and press ENTER

m) On the Processing Options Panel, enter Y for Explode RACF groups in access
list at end of report? and Explode Users/Groups in Surrogate ID access list at
end of report? Press ENTER

n) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

o) Save the output for use in the
localnodeid.JES2.$TRCLOG.taskid.*.JESTRACE
check.

p) On the General Resources Reports panel, enter localnodeid.+MASTER+.* in the
Profile field, enter JESSPOOL in the Class field and enter B for Batch/Online.
Select option 4 Access Lists and press ENTER

q) On the Processing Options Panel, enter Y for Explode RACF groups in access

list at end of report? and Explode Users/Groups in Surrogate ID access list at
end of report? Press ENTER

r) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

s) Save the output for use in the
localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG* checks.

t) Ensure that access authorization for the following resources:

localnodeid.JES2.$TRCLOG.taskid.*.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG or
localnodeid.+BYPASS+.SYSLOG.jobid.-.SYSLOG

is restricted to the following:

1. Userid(s) associated with external writer(s)

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.

3. Application Development and Application Support personnel responsible for
diagnosing application problems can have READ access to the SYSLOG resource

u) If item (t) is true, there is NO FINDING.

v) If item (t) is untrue, this is a FINDING

Fix Text: The IAO will ensure that access authorization for resources defined to
the JESTRACE and SYSLOG resources in the JESSPOOL resource class is restricted
to the appropriate personnel.

Review the following resources defined to the JESSPOOL resource class:

Ensure the following resources are defined to the JESSPOOL resource class with a
UACC(NONE):

localnodeid.JES2.$TRCLOG.taskid.*.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG or

```
localnodeid.+BYPASS+.SYSLOG.jobid.*.SYSLOG

NOTE:       These resource profiles may be more generic as long as they
pertain
directly to the JESTRACE and SYSLOG data sets. For example:

localnodeid.JES2.$TRCLOG.*.**
localnodeid.+MASTER+.SYSLOG.*.** or
localnodeid.+BYPASS+.SYSLOG.*.**

NOTE:       Review the JES2 parameters to determine the localnodeid by
searching
for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn)
(where
nnnn is the value specified by OWNNODE). The NAME parameter value
specified on
this NODE statement is the localnodeid. Another method is to issue the
JES2
command $D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

Ensure that access authorization for the resources mentioned above is
restricted
to the following:

Userid(s) associated with external writer(s) can have complete access.

NOTE:       An external writer is a STC that removes data sets from the
JES
spool. In this case, it is responsible for archiving the JESTRACE and
SYSLOG
data sets. The STC default name is XWTR and the external writer program
is
called IASXWR00.

Systems personnel and security administrators responsible for diagnosing
JES2
and z/OS problems can have complete access.

Application Development and Application Support personnel responsible for
diagnosing application problems can have READ access to the SYSLOG
resource.

Examples:

RDEFINE JESSPOOL localnodeid.JES2.$TRCLOG.*.** audit(failures(read))
uacc(NONE)
-
data('Reference srr finding ZJES0044 ') owner(admin)

RDEFINE JESSPOOL localnodeid.+MASTER+.SYSLOG.*.** audit(failures(read))
uacc(NONE) -
data('Reference srr finding ZJES0044') owner(admin)
or
RDEFINE JESSPOOL localnodeid.+BYPASS+.SYSLOG.*.** audit(failures(read))
```

```
uacc(NONE) -
data('Reference srr finding ZJES0044') owner(admin)

PE localnodeid.JES2.$TRCLOG.** cl(jesspool) id(<syspaudt> <secaaudt>)
acc(a)
PE localnodeid.+MASTER+.SYSLOG.*.** cl(jesspool) id(<syspaudt>
<secaaudt>)
acc(a)
PE localnodeid.+MASTER+.SYSLOG.*.** cl(jesspool) id(<appdpaudt>
<appsaudt>)
acc(r)
or
PE localnodeid.+BYPASS+.SYSLOG.*.** cl(jesspool) id(<syspaudt>
<secaaudt>)
acc(a)
PE localnodeid.+BYPASS+.SYSLOG.*.** cl(jesspool) id(<appdpaudt>
<appsaudt>)
acc(r)
```

CCI: CCI-000213

CCI: CCI-001762

Group ID (Vulid): V-223753
Group Title: JS000090
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000090
Rule Title: JES2 spool resources will be controlled in accordance with security
requirements.

Vulnerability Discussion: JES2 spool resources include all SYSOUT, SYSLOG,
JESTRACE, and JESNEWS data sets. Failure to properly control JES2 spool
resources could result in unauthorized personnel accessing job output, system
activity logs, and trace data containing userid and password information. This
exposure may threaten the integrity and availability of the operating system
environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Use the list of NJE nodes from ZJES012 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.

b) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

c) Select option 4 General Resource Profile

d) In all profile names, replace localnodeid with the NAME parameter from the
node determined as OWNNODE in step a.

e) On the General Resources Reports panel, enter localnodeid.* in the Profile
field,
enter JESSPOOL in the Class field and enter B for Batch/Online. Select option 4
Access Lists and press ENTER

f) On the Processing Options Panel, enter Y for Explode RACF groups in access
list at end of report? and Explode Users/Groups in Surrogate ID access list at
end of report? Press ENTER

g) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

h) Save the output for use in the
localnodeid.userid.jobname.jobid.dsnumber.name
check #1.

i) On the General Resources Reports panel, enter localnodeid.* in the Profile
field,
enter JESSPOOL in the Class field and enter B for Batch/Online. Select option 2
Audit Flags and press ENTER

j) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

k) Save the output for use in the
localnodeid.userid.jobname.jobid.dsnumber.name
check #3.

l) Review the output from steps h and k for resource profiles with the following
naming convention. These profiles may be fully qualified as indicated below or
generic:

* 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 RACF 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 (?).

m) If the resources described in (l) are not present, there is NO FINDING.

n) If the resources described in (l) are present, ensure the following items are in effect:

1. All users shall have access to their own JESSPOOL resources. This resource access does not require logging.
2. The resource localnodeid.** will be restricted to only system programmers, operators and automated operations personnel, with access of ALTER. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc)
3. 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. UPDATE, CONTROL, and ALTER 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.
4. 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.
5. 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. All access will be logged.

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

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

Fix Text: The IAO will develop a plan of action to implement the required changes. Ensure the following items are in effect for JESSPOOL resources. The
JESSPOOL may have more restrictive security at the direction of the IAO.

The JESSPOOL resources may be fully qualified, be specified as generic, or be
specified with masking as indicated below:

localnodeid.userid.jobname.jobid.dsnumber.name

localnodeid The name of the node on which the SYSIN or SYSOUT data set
currently resides.

userid The userid associated with the job. This is the userid used
for validation purposes when the job runs.

jobname The name that appears in the name field of the JOB statement.

jobid The job number JES2 assigned to the job.

dsnumber The unique data set number JES2 assigned to the spool data
set. A D is the first character of this qualifier.

name The name of the data set specified in the DSN= parameter of the
DD statement. If the JCL did not specify DSN= on the DD statement that creates
the spool data set, JES2 uses a question mark (?).

By default a user has access only to that user s own JESSPOOL resources. However, situations exist where a user legitimately requires access to jobs that
run under another user s userid. In particular, if a user routes SYSOUT to an
external writer, the external writer should have access to that user s SYSOUT.

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel with access of ALTER. All access
will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc)

```
RDEF JESSPOOL localnodeid.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('PROTECT JESSPOOL AT HIGH LEVEL, REF ZJES0046')
PE localnodeid.** CL(JESSPOOL) ID(syspaudt) ACC(A)
```

The JESSPOOL localnodeid.userid.jobname.jobid.dsnumber.name, whether generic
and/or masked, can be made available to users, when approved by the IAO. Access
will be identified at the minimum access for the user to accomplish the users
function, SERVICE(READ, UPDATE, DELETE, ADD). All access will be logged. An
example is team members within a team, providing the capability to view, help,
and/or debug other team member jobs/processes. If frequent situations occur
where users working on a common project require selective access to each other's
jobs, then the installation may delegate to the individual users the authority
to grant access, but only with the approval of the IAO.

```
RDEF JESSPOOL localnode.userid.jobname.jobid.dsnumber.name
UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('PROTECT JESSPOOL, REF ZJES0046')
PE localnode.userid.jobname.jobid.dsnumber.name CL(JESSPOOL)
ID(<users_or_groups>) ACC(R)
```

If IBM s SDSF product is installed on the system, resources defined to the
JESSPOOL resource class control functions related to jobs, output groups, and
SYSIN/SYSOUT data sets on various SDSF panels.

CSSMTP will not be granted to the JESSPOOL resource of the high level node. or
localnodeid. . CSSMTP can have access to the specific approved JESSPOOL
resources, minimally qualified to the node.userid. and all access will be
logged. This will ensure system records who (userid) sent traffic to CSSMTP,
when and what job/process.

Spooling products users (CA-SPOOL, CA View, etc.) will be restricted to
localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked
when approved by the IAO. Logging of access is not required.

The IAO will review JESSPOOL resource rules. If a rule has been determined not
to have been used within the last 2 years, the rule shall be removed.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223754
Group Title: JS000100
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000100
Rule Title: JES2 system commands are not protected in accordance with security
requirements.

Vulnerability Discussion: JES2 system commands are used to control JES2 resources and the operating system environment. Failure to properly control
access to JES2 system commands could result in unauthorized personnel issuing
sensitive JES2 commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) From Administrator main Menu, select option 9 Analyzer. Press ENTER

b) From Analyzer main menu, select 4 Batch Reports. Press ENTER
c) From Batch Reports menu, select F Subsystem Name Table Analysis. Press ENTER

d) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press ENTER

e) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press ENTER

f) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

g) Review the output. Note that the first entry in the report is the JES2 subsystem
name and is typically JES2. This will be used in step j.

h) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

i) Select option 4 General Resource Profile

j) In all profile names, replace JES2 with the JES2 subsystem name determined in
step g.

k) On the General Resources Reports panel, enter JES2.* in the Profile field,

enter
OPERCMDS in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press ENTER

l) On the Processing Options Panel, enter Y for Explode RACF groups in access
list at end of report? and Explode Users/Groups in Surrogate ID access list at
end of report? Press ENTER

m) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

n) Save the output for use in the JES2.* access list check.

o) On the General Resources Reports panel, enter JES2.* in the Profile field,
enter
OPERCMDS in the Class field and enter B for Batch/Online. Enter 2 on the command line to select Audit Flags and Press ENTER
p) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

q) Save the output for use in the JES2.* audit check.

r) On the General Resources Reports panel, enter JES2.* in the Profile field,
enter
OPERCMDS in the Class field and enter B for Batch/Online. Press ENTER

s) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

t) Save the output for use in the JES2.* UACC check.

u) If the JES2.** resource is defined to the OPERCMDS class with a default
access
of NONE and all access is logged, there is NO FINDING.

v) 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 Auth category specified in the table below as a guideline to determine appropriate personnel access to system commands.

w) 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 as indicated in the LOG column, there is NO FINDING.

x) If either (b), (c), or (d) above is untrue for any JES2 system command resource, this is a FINDING.

Fix Text: Extended MCS support allows the installation to control the use of JES2 system commands through the ACP. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

To control access to JES2 system commands, apply the following recommendations when implementing security:

1) Define the JES2.** resource in the OPERCMDS class with a default access of NONE and all access is logged.

2) Define the JES2 system commands as specified in the "Controls on JES2 System Commands" table, in the zOS STIG Addendum restricts access to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

3) Define the JES2 system commands with proper logging as specified in the "Controls on JES2 System Commands" table, in the zOS STIG Addendum.

Build a command file based on the referenced JES2 Command Table. A sample of the
commands in the command file is provided here:

```
RDEF OPERCMDS JES2.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('REQUIRED BY
SRR PDI ZJES0052')

RDEF OPERCMDS JES2.<command>.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('REQUIRED BY SRR PDI ZJES0052')
PE JES2.<command>.** CL(OPERCMDS) ID(<syspaudt>) ACC(U)

SETR RACL(OPERCMDS) REF
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223755
Group Title: JS000110
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000110
Rule Title: Surrogate users must be controlled in accordance with proper security requirements.

Vulnerability Discussion: Surrogate users have the ability to submit jobs on
behalf of another user (the execution user) without specifying the execution
user's password. Jobs submitted by surrogate users run with the identity of the
execution user. Failure to properly control surrogate users could result in
unauthorized personnel accessing sensitive resources. This exposure may threaten
the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

b) Select option 4 General Resource Profile

c) On the General Resources Reports panel, enter *.SUBMIT in the Profile field,
enter SURROGAT in the Class field and enter B for Batch/Online. Select option
4 Access Lists and press ENTER

d) On the Processing Options Panel, enter Y for Explode RACF groups in access
list at end of report? and Explode Users/Groups in Surrogate ID access list at
end of report? Press ENTER

e) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

f) Save the output for use in the executionuserid.SUBMIT access list check.

g) On the General Resources Reports panel, enter *.SUBMIT in the Profile field,
enter SURROGAT in the Class field and enter B for Batch/Online. Enter 2 on the
command line to select Audit Flags and press ENTER

h) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

i) Save the output for use in the executionuserid.SUBMIT audit check.

j) On the General Resources Reports panel, enter *.SUBMIT in the Profile field,
enter SURROGAT in the Class field and enter B for Batch/Online. Press ENTER

k) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

l) Save the output for use in the executionuserid.SUBMIT UACC check.

m) If no executionuserid.SUBMIT resources are defined to the SURROGAT resource class, there is NO FINDING.

n) If executionuserid.SUBMIT resources are defined to the SURROGAT resource
class, ensure the following items are in effect regarding surrogate controls:

o) All executionuserid.SUBMIT resources defined to the SURROGAT resource class specify a default access of NONE.

p) All resource access is except for scheduling tasks.

q) Access authorization is restricted to scheduling tools, started tasks or other applications required for running production jobs.

r) 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).

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

t) If any item in (n) is untrue, this is a FINDING.

Fix Text: For executionuserid.SUBMIT resources defined to the SURROGAT resource class, ensure the following items are in effect regarding surrogate controls:

All executionuserid.SUBMIT resources defined to the SURROGAT resource class specify a default access of NONE.

All resource access is logged except for scheduling tasks. This is optional and the ISSM/ISSO scheduling tasks may be exempted.
Access authorization is restricted to scheduling tools, started tasks or other system applications required for running production jobs.

Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent).

Consider the following recommendations when implementing security for Surrogate Users:

Keep the use of Surrogate Users outside of those granted to the scheduling software to a minimum number of individuals.
The simplest configuration is to only use Surrogate resource for the appropriate Scheduling task/software for production scheduling purposes as documented.

Temporary use of surrogate resource of the production batch to the scheduling

tasks may be allowed for a period for testing by the appropriate specific production Support Team members. Authorization, eligibility and test period is
determined by site policy.

Access authorization is restricted to the minimum number of personnel required
for running production jobs. However, Surrogate usage should not become the
default for all jobs submitted by individual userids (i.e., system programmer
shall use their assigned individual userids for software installation, duties,
whereas a Cross Authorized ACID would normally be utilized for scheduled batch
production only and as such shall normally be limited to the scheduling task
such as CONTROLM) and not granted as a normal daily basis to individual users..

Command samples are provided to define/permit SURROGAT profiles:

```
SETR CLASSACT(SURROGAT)
SETR GENERIC(SURROGAT) GENCMD(SURROGAT)
SETR RACL(SURROGAT)

RDEF SURROGAT <batchid>.SUBMIT UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('SUBMIT JOBS FOR <batchid>, REFERENCE ZJES0060')

PE <batchid>.SUBMIT CL(SURROGAT) ID(<authorized user such as CONTROLM>)
```

CCI: CCI-000213

CCI: CCI-002233

CCI: CCI-002234

Group ID (Vulid): V-98219
Group Title: JS000120
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): JS000120
Rule Title: RJE workstations and NJE nodes are not controlled in accordance with
security 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.

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

Check Content:
Note that this guidance addresses RJE Workstations that are "Dedicated". If an
RJE
workstation is dedicated, the assumption is that the RJE to host connection is
hard-wired
between the RJE and host. In this case the RMT definition statement will contain
the
keyword LINE= which specifies that this RJE is only connected via that one LINE
statement.

a) Determine the JES2PARM member as specified in the HASPPARM DD of the
PROCLIB member used to start JES2.

b) Review the workstation definitions by searching for RMT(in the member).
c) From Administrator main Menu, select option 3 Security Server Reports; Press
ENTER

d) Select option 1 User Profile. Change the * next to User ID to RMT* and press
ENTER

e) Print the screen(s) for use in check #1.

f) Perform the following for each RJE workstation found:

g) Enter LR command next to each userid on your list. Press ENTER

h) Save the name of the dataset being browsed. Split screen, select option 1,
and
view the dataset from step h. Save it to your documentation library PDS. Note
the PDS name and member name for use in check #2. Close the view session.

i) Press <PF3> to get to the next userid and repeat the process from step h.
When
all userids have been processed, you will be returned to the userid list. Press
<PF3> once more to return to Security Server Reports.

j) Select option 17 ID in Access List. Press ENTER

k) Select option 1 ID in Access List. Enter U next to ID Type, enter RMT* for ID
Name, and enter B for Batch/Online. Press ENTERtwice

l) On the JCL Submit Processing panel, enter E on the command line.

m) Change the REGION parameter on the execute card to 0M. Press <PF3>

n) On the JCL Submit Processing panel, enter S on the command line to submit the
job. Press ENTER

o) Save the output
p) For each RJE workstation definition found by searching for RMT(in step b
perform the following:
1. A userid of RMTnnnn is defined to RACF for each RJE workstation,
where nnnn is the number on the RMT statement (review output from
step e)
2. No userid segments (e.g., TSO, CICS, etc.) are defined (review output from step h)
3. Restricted from accessing all data sets and resources (review output from
step o).
4. NOTE: If no RJE workstations are defined to JES2, this is NOT APPLICABLE.

q) If all of (p) is true, there is NO FINDING.

r) If any of (p) is untrue, this is a FINDING.

Fix Text: RJE Userids

Note that this guidance addresses RJE Workstations that are "Dedicated". If an
RJE workstation is dedicated, the assumption is that the RJE to host connection
is hard-wired between the RJE and host. In this case the RMT definition
statement will contain the keyword LINE= which specifies that this RJE is only
connected via that one LINE statement.

There are no known non-dedicated RJE Workstations in use within CSD. If such

devices are used, the site should open a ticket with the FSO and jointly develop
proper security controls.

a) Review the JES2 parameters for RJE workstation definitions by searching
for RMT(in the report.

b) Ensure the RJE workstation userids are defined as follows:

1) A userid of RMTnnnn is defined to RACF for each RJE workstation, where
nnnn is the number on the RMT statement.

2) No userid segments (e.g., TSO, CICS, etc.) are defined.

3) Restricted from accessing all data sets and resources with exception of
the corresponding JESINPUT-class profile for that remote.

Review Chapter 17 of the RACF Security Admin Guide. The following is an example
that show proper implementation:

```
AG RMTGRP OWNER(ADMIN) SUPGROUP(ADMIN)

AU RMT777 NAME('RMT RJE 777') DFLTGRP(RMTGRP) OWNER(RMTGRP) DATA('COMPLY WITH
ZJES0011') NOPASS RESTRICTED

PE RMT777 CL(JESINPUT) ID(RMT777)
```

c) Ensure that a FACILITY-Class profile exists in the format RJE.RMTnnnn
where nnn identifies the remote number.

A command example is shown here:

```
RDEF FACILITY RJE.RMT777 UACC(NONE) OWNER(ADMIN) DATA('COMPLY WITH
ZJES0011 FOR
RJE 777')
```

CCI: CCI-000366

Group ID (Vulid): V-223757
Group Title: OS000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000010
Rule Title: Non-standard SMF data collection options specified.

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

Documentable: YES
Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECAR-3

Check Content:
a) From Analyzer main Menu, go to 3;L;<ENTER>

b) Place a B next to the first occurrence of SMFPRMnn

c) If all the options for SMF data gathering are set as required (in the table
shown at
the end of this STIG) there is NO FINDING.

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

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

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

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

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

f) The IAM may set selected userids to have a time-out of up to 60 minutes in

order
to complete critical reports or transactions without timing out. Each exception
must meet the following criteria:

The time-out exception cannot exceed 60 minutes.

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

The requirement must be revalidated on an annual basis.

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

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

ACTIVE: Activates the collection of SMF data.

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

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

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

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

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

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

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

SYS(NOTYPE) indicates that the supplied list

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

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

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

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

ACTIVE Activates the collection of SMF data.

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

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

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

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

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

(a) The time-out exception cannot exceed 60 minutes.

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

MAXDORM(0500) Specifies the amount of real time that SMF allows data to remain in an SMF buffer before it is written to a recording data set.
SID Specifies the system ID to be recorded in all SMF records

SYS(DETAIL) Controls the level of detail recorded.

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

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

CCI: CCI-000057

CCI: CCI-000130

CCI: CCI-001844

CCI: CCI-001851

Group ID (Vulid): V-223758
Group Title: OS000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000020
Rule Title: The IBM z/OS BPX.SMF resource must be properly configured.

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Responsibility: N/A
IAControls: N/A

Check Content:
a) Using Vanguard Administrator select Security Server Reports
b) select Option 4 General Resource Profile

c) Type FACILITY in the class field and hit enter
CDT Classes:..... _ (E to edit data) *data is present*
Review the FACILITY resource class for BPX.SMF.

If the RACF rules are as follows this is not a finding.

BPX.SMF.119.94 READ allowed for users running the ssh, sftp, or scp client commands.
BPX.SMF.119.96 READ allowed for users running the scp or sftp-server server commands.
BPX.SMF.119.97 READ allowed for users running the scp or sftp client commands.

The following profile grants the permitted users the authority to write or test for any SMF record being recorded. Access should be permitted as follows:
BPX.SMF READ access only when documented and justified in Site Security Plan.
Documentation should include a reason why a more specific profile is not

acceptable.

Fix Text: a) Using Vanguard Administrator select Security Server Commands
b) select Option 4 General Resource Profile
c) Type FACILITY in the class field and as example(BPX.SMF.119.94) and hit enter
d) respond Y to Display covering profile
e)If there is a covering profile you are ok
f)if not configure profile from next panel
Configure Facility resource class for BPX.SMF as follows:
BPX.SMF.119.94 READ allowed for users running the ssh, sftp, or scp client
commands.
BPX.SMF.119.96 READ allowed for users running the scp or sftp-server server
commands.
BPX.SMF.119.97 READ allowed for users running the scp or sftp client
commands.

The following profile grants the permitted users the authority to write or test
for any SMF record being recorded. Access should be permitted as follows:
BPX.SMF READ access only when documented and justified in Site Security Plan.
Documentation should include a reason why a more specific profile is not acceptable.

CCI: CCI-000067

Group ID (Vulid): V-223759
Group Title: OS000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000030
Rule Title: SMF recording options for the TN3270 Telnet Server must be properly
specified.

Vulnerability Discussion: The TN3270 Telnet Server can provide audit data in
the form of SMF records. The SMF data produced provides information about
individual sessions. This data includes the VTAM application, the remote and
local IP addresses, and the remote and local IP port numbers. Failure to collect
and retain audit data may contribute to the loss of accountability and hamper
security audit activities.

Responsibility: Systems Programmer

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

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
TELNETPARMS SMFINIT and SMFTERM statements are coded with the STD operand within each TELNETPARMS statement block.

a) Using SDSF or equivalent, locate the Profile configuration file specified on the
PROFILE DD statement in the TCPIP started task JCL or the TN3270 started task
if configured separately in z/OS 1.8 and above.

b) Using IBM s utility Dslist or equivalent locate the Profile configuration
file and
browse to review the file.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

c) Ensure the following item is in effect for the configuration statements
specified in
the Profile configuration file:
-The TELNETPARMS SMFINIT and SMFTERM statements are coded with the STD operand within each TELNETPARMS statement block.

NOTE: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

d) If the above is true, there is NO FINDING.

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

Fix Text: The system programmer responsible for the IBM Communications Server
will review the TELNETPARMS SMFINIT and SMFTERM statements in the PROFILE.TCPIP
file. Ensure they conform to the requirements specified below.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

The TELNETPARMS SMFINIT statement is coded with the TYPE119 operand within each

TELNETPARMS statement block.

The TELNETPARMS SMFTERM statement is coded with the TYPE119 operand within each
TELNETPARMS statement block.

NOTE: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can
appear in both TELNETGLOBAL and TELNETPARM statement blocks.

CCI: CCI-000130

Group ID (Vulid): V-223760
Group Title: OS000040
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): OS000040
Rule Title: IBM RACF must be installed and active on the system.

Vulnerability Discussion: Enterprise environments make account management for
operating systems challenging and complex. A manual process for account management functions adds the risk of a potential oversight or other errors. IBM
z/OS requires an external security manager to assure proper account management.

Responsibility: N/A
IAControls: N/A

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper IEFSSnxx member.

If RACF is defined in the SubSystem member, this is not a finding.

Fix Text: Refer to the IBM Security Server RACF System Programmer Guide and the
IBM Security Server RACF Security Administrator guide to properly implement RACF
on the system.

CCI: CCI-000015

Group ID (Vulid): V-223761
Group Title: OS000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000050

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to disable emergency accounts after the crisis is resolved or 72 hours.

Vulnerability Discussion: Emergency accounts are privileged accounts that are established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the documented process to disable emergency accounts.

If there is no documented process, this is a finding.

Examine the process, if it does not include procedures to disable emergency accounts after the crisis is resolved or 72 hours, this is a finding.

Fix Text:
Develop a process to disable emergency accounts after the crisis is resolved or
72 hours.

CCI: CCI-001682

Group ID (Vulid): V-223762
Group Title: OS000060
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000060
Rule Title: The IBM z/OS System Administrator (SA) must develop a process to
notify appropriate personnel when accounts are created.

Vulnerability Discussion: Once an attacker establishes access to a system, the
attacker often attempts to create a persistent method of reestablishing access.
One way to accomplish this is for the attacker to create a new account.
Notification of account creation is one method for mitigating this risk. A
comprehensive account management process will ensure an audit trail which
documents the creation of operating system user accounts and notifies
administrators and ISSOs that it exists. Such a process greatly reduces the risk
that accounts will be surreptitiously created and provides logging that can be
used for forensic purposes.

To address access requirements, many operating systems can be integrated with
enterprise-level authentication/access/auditing mechanisms that meet or exceed
access control policy requirements.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:
Ask the system Administrator for the documented process to notify appropriate
personnel when accounts are created.

If there is no documented process, this is a finding.

Fix Text: Develop a documented develop a process to notify appropriate personnel
when accounts are created.

CCI: CCI-000764

Group ID (Vulid): V-223763
Group Title: OS000070
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000070
Rule Title: The IBM z/OS System Administrator (SA) must develop a process to
notify appropriate personnel when accounts are modified.

Vulnerability Discussion: Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and
manipulate audit information system activity and records. Audit tools include
custom queries and report generators.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system Administrator for the documented process to notify appropriate
personnel when accounts are modified.

If there is no documented process, this is a finding.

Fix Text:
Develop a documented develop a process to notify appropriate personnel when
accounts are modified.

CCI: CCI-001684

Group ID (Vulid): V-223764
Group Title: OS000080
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000080
Rule Title: The IBM z/OS System Administrator (SA) must develop a process to
notify appropriate personnel when accounts are deleted.

Vulnerability Discussion: Audit tools include, but are not limited to,

vendor-provided and open source audit tools needed to successfully view and
manipulate audit information system activity and records. Audit tools include
custom queries and report generators.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system Administrator for the documented process to notify appropriate
personnel when accounts are deleted.

If there is no documented process, this is a finding.

Fix Text:
Develop a documented develop a process to notify appropriate personnel when
accounts are deleted.

CCI: CCI-001685

Group ID (Vulid): V-223765
Group Title: OS000090
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000090
Rule Title: The IBM z/OS System Administrator (SA) must develop a process to
notify appropriate personnel when accounts are removed.

Vulnerability Discussion: When operating system accounts are removed, user
accessibility is affected. Accounts are utilized for identifying individual
operating system users or for identifying the operating system processes
themselves. Sending notification of account removal events to the system
administrator and ISSO is one method for mitigating this risk. Such a capability
greatly reduces the risk that operating system accessibility will be negatively
affected for extended periods of time and also provides logging that can be used
for forensic purposes.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system Administrator for the documented process to notify appropriate
personnel when accounts are removed.

If there is no documented process, this is a finding.

Fix Text:
Develop a documented develop a process to notify appropriate personnel when
accounts are removed.

CCI: CCI-001686

Group ID (Vulid): V-223766
Group Title: OS000100
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000100
Rule Title: The IBM z/OS System Administrator (SA) must develop a process to
notify Information System Security Officers (ISSOs) of account enabling actions.

Vulnerability Discussion: Once an attacker establishes access to a system, the
attacker often attempts to create a persistent method of reestablishing access.
One way to accomplish this is for the attacker to enable an existing disabled
account. Sending notification of account enabling actions to the system
administrator and ISSO is one method for mitigating this risk. Such a capability
greatly reduces the risk that operating system accessibility will be negatively
affected for extended periods of time and also provides logging that can be used
for forensic purposes.

In order to detect and respond to events that affect user accessibility and
application processing, operating systems must audit account enabling actions
and, as required, notify the appropriate individuals so they can investigate the
event.

To address access requirements, many operating systems can be integrated with

enterprise-level authentication/access/auditing mechanisms that meet or exceed
access control policy requirements.

Responsibility: System Administrator (
IAControls: N/A

Check Content:

Ask the system Administrator for the documented processes to notify the Information System Security Officers (ISSOs) of account enabling actions.

If there is no documented process, this is a finding.

Fix Text:
Develop a documented process to notify the Information System Security Officers
(ISSOs) of account enabling actions.

CCI: CCI-002132

Group ID (Vulid): V-223767
Group Title: OS000110
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000110
Rule Title: Required SMF data record types must be collected.

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

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

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

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

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

0 (00) IPL
6 (06) External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) [SMF] Data Lost
14 (0E) INPUT or RDBACK Data Set Activity
15 (0F) OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) Scratch Data Set Status
18 (12) Rename Non-VSAM Data Set Status
24 (18) JES2 Spool Offload
25 (19) JES3 Device Allocation
26 (1A) JES Job Purge
30 (1E) Common Address Space Work
32 (20) TSO/E User Work Accounting
41 (29) DIV Objects and VLF Statistics
42 (2A) DFSMS statistics and configuration
43 (2B) JES Start
45 (2D) JES Withdrawal/Stop
47 (2F) JES SIGNON/Start Line (BSC)/LOGON
48 (30) JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) JES Integrity
52 (34) JES2 LOGON/Start Line (SNA)
53 (35) JES2 LOGOFF/Stop Line (SNA)
54 (36) JES2 Integrity (SNA)
55 (37) JES2 Network SIGNON
56 (38) JES2 Network Integrity
57 (39) JES2 Network SYSOUT Transmission
58 (3A) JES2 Network SIGNOFF
60 (3C) VSAM Volume Data Set Updated
61 (3D) Integrated Catalog Facility Define Activity
62 (3E) VSAM Component or Cluster Opened
64 (40) VSAM Component or Cluster Status
65 (41) Integrated Catalog Facility Delete Activity
66 (42) Integrated Catalog Facility Alter Activity
80 (50) RACF/TOP SECRET Processing
81 (51) RACF Initialization
83 (53) RACF Audit Record For Data Sets
90 (5A) System Status
92 (5C) except subtypes 10, 11 OpenMVS File System Activity
102 (66) DATABASE 2 Performance
103 (67) IBM HTTP Server
110 (6E) CICS/ESA Statistics
118 (76) TCP/IP Statistics
119 (77) TCP/IP Statistics
199 (C7) TSOMON
230 (E6) ACF2 or as specified in ACFFDR (vendor-supplied default is 230)

231 (E7) TSS logs security events under this record type

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

IBM SMF Records to be collect at a minimum

0 (00) IPL
6 (06) External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) [SMF] Data Lost
14 (0E) INPUT or RDBACK Data Set Activity
15 (0F) OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) Scratch Data Set Status
18 (12) Rename Non-VSAM Data Set Status
24 (18) JES2 Spool Offload
25 (19) JES3 Device Allocation
26 (1A) JES Job Purge
30 (1E) Common Address Space Work
32 (20) TSO/E User Work Accounting
41 (29) DIV Objects and VLF Statistics
42 (2A) DFSMS statistics and configuration
43 (2B) JES Start
45 (2D) JES Withdrawal/Stop
47 (2F) JES SIGNON/Start Line (BSC)/LOGON
48 (30) JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) JES Integrity
52 (34) JES2 LOGON/Start Line (SNA)
53 (35) JES2 LOGOFF/Stop Line (SNA)
54 (36) JES2 Integrity (SNA)
55 (37) JES2 Network SIGNON
56 (38) JES2 Network Integrity
57 (39) JES2 Network SYSOUT Transmission
58 (3A) JES2 Network SIGNOFF
60 (3C) VSAM Volume Data Set Updated
61 (3D) Integrated Catalog Facility Define Activity
62 (3E) VSAM Component or Cluster Opened
64 (40) VSAM Component or Cluster Status
65 (41) Integrated Catalog Facility Delete Activity
66 (42) Integrated Catalog Facility Alter Activity
80 (50) RACF/TOP SECRET Processing
81 (51) RACF Initialization
83 (53) RACF Audit Record For Data Sets
90 (5A) System Status
92 (5C) except subtypes 10, 11 OpenMVS File System Activity
102 (66) DATABASE 2 Performance
103 (67) IBM HTTP Server
110 (6E) CICS/ESA Statistics
118 (76) TCP/IP Statistics
119 (77) TCP/IP Statistics
199 (C7) TSOMON
230 (E6) ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
231 (E7) TSS logs security events under this record type

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000169

CCI: CCI-000172

CCI: CCI-001353

CCI: CCI-001487

Group ID (Vulid): V-223768
Group Title: OS000120
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000120
Rule Title: IBM z/OS must employ a session manager to manage display of the
Standard Mandatory DoD Notice and Consent Banner.

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and
security notification verbiage used is consistent with applicable federal laws,
Executive Orders, directives, policies, regulations, standards, and guidance.
All methods of gaining access to the system must comply with this requirement to
assure that regulations are upheld.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Verify that any session manger in use displays the Standard Mandatory DoD Notice
and Consent Banner before granting access to the system.

If the session manager does not display the Standard Mandatory DoD Notice and
Consent Banner before granting access to the system, this is a finding.

Fix Text:
Configure any session manger in use to display the Standard Mandatory DoD Notice
and Consent Banner before granting access to the system.

CCI: CCI-000048

Group ID (Vulid): V-223769
Group Title: OS000130
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000130
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.

Responsibility: Information Assurance Officer
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-223770
Group Title: OS000140
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000140
Rule Title: IBM z/OS SMF collection files (system MANx datasets or LOGSTREAM
DASD) must have storage capacity to store at least one weeks worth of audit
data.

Vulnerability Discussion: In order to ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems
need to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during
initial installation of the operating system.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Review the SMF dump procedure in there system.

If the output datasets in the procedure have storage capacity to store at least
one week's worth of audit data, this is not a finding.

Fix Text:
Make sure output file and dump procedures allow storage capacity to store one
week's worth of audit data.

CCI: CCI-001849

Group ID (Vulid): V-223771
Group Title: OS000150
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000150
Rule Title: IBM z/OS system administrators must develop an automated process to
collect and retain SMF data.

Vulnerability Discussion: Information stored in one location is vulnerable to
accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:

Ask the system administrator if there is an automated process is in place to
collect and retain all SMF data produced on the system.

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,
this is not a finding.

If it cannot be determined this process exists and is being adhered to, this is
a finding.

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

Review SMF data collection and retention processes. Develop processes are 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:

-Dump each SMF file as it fills up during the normal course of daily processing
-Dump all remaining SMF data at the end of each processing day or
-Establish a process using Audit logging

CCI: CCI-001851

Group ID (Vulid): V-223772
Group Title: OS000160
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000160
Rule Title: IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.

Vulnerability Discussion: It is critical for the appropriate personnel to be
aware if a system is at risk of failing to process audit logs as required.
Without this notification, the security personnel may be unaware of an impending
failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the
audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct
information system component where audit records are stored), the centralized
audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member in SYS1.PARMLIB.

If BUFUSEWARN is set for "75" (75%) or less, this is not a finding.

Fix Text:
Configure the BUFUSEWARN statement in SMFPRMxx to "75" (75%) or less.

CCI: CCI-000139

CCI: CCI-001855

CCI: CCI-001858

Group ID (Vulid): V-223773
Group Title: OS000170
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000170
Rule Title: IBM z/OS NOBUFFS in SMFPRMxx must be properly set (default is MSG).

Vulnerability Discussion: It is critical that when the operating system is at
risk of failing to process audit logs as required, it takes action to mitigate
the failure. Audit processing failures include: software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being
reached or exceeded. Responses to audit failure depend upon the nature of the
failure mode.

When availability is an overriding concern, other approved actions in response
to an audit failure are as follows:

If the failure was caused by the lack of audit record storage capacity, the
operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the
oldest audit records in a first-in-first-out manner.

If audit records are sent to a centralized collection server and communication

with this server is lost or the server fails, the operating system must queue
audit records locally until communication is restored or until the audit records
are retrieved manually. Upon restoration of the connection to the centralized
collection server, action should be taken to synchronize the local audit data
with the collection server.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member in SYS1.PARMLIB.

If NOBUFFS is set to "HALT", this is not a finding.

Note: If availability is an overriding concern NOBUFFS can be set to MSG.

Fix Text:
Configure NOBUFFS to "HALT" unless availability is an overriding concern then
NOBUFFS can be set to MSG.

CCI: CCI-000140

Group ID (Vulid): V-223774
Group Title: OS000180
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000180
Rule Title: The IBM z/OS SNTP daemon (SNTPD) must be active.

Vulnerability Discussion: Inaccurate time stamps make it more difficult to
correlate events and can lead to an inaccurate analysis. Determining the correct
time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time
stamps for information systems with multiple system clocks and systems connected
over a network.

Organizations should consider endpoints that may not have regular access to the
authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

From UNIX System Services ISPF Shell navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SNTP Daemon (SNTPD) is not active, this is a finding.

Fix Text:
Obtain a copy of this sample procedure from SEZAINST and store it in one of your
PROCLIB concatenation data sets.

Perform the following step to start SNTPD as a procedure:
Invoke the procedure using the system operator start command. The following
sample, SEZAINST(SNTPD), shows how to start SNTPD as a procedure:

```
//*
//* Sample procedure for the Simple Network Time Protocol (SNTP)
//*
//* z/OS Communications Server Version 1 Release 13
//* SMP/E Distribution Name: SEZAINST(EZASNPRO)
//*
//* Copyright: Licensed Materials - Property of IBM
//* 5650-ZOS
//* Copyright IBM Corp. 2002, 2015
//*
//* Status: CSV2R2
//*
//SNTPD EXEC PGM=SNTPD,REGION=4096K,TIME=NOLIMIT,
//PARM= / -d
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=132,BLKSIZE=132)
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*,DCB=(RECFM=F,LRECL=132,BLKSIZE=132)
//CEEDUMP DD SYSOUT=*
//SYSABEND DD SYSOUT=*
```

CCI: CCI-001891

Group ID (Vulid): V-223775
Group Title: OS000190
Rule ID: N/A

Severity: CAT II
Rule Version (STIG-ID): OS000190
Rule Title: IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time, a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

From the ISPF Command Shell enter:
cd /usr/sbin
ls -al

If the following File permission and user Audit Bits are true, this is not a finding.

/usr/sbin/sntpd 1740 faf

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:
With the assistance of a systems programmer with UID(0) and/or SUPERUSER access,
configure the UNIX permission bits and user audit bits on the SNTPD to conform
to the specifications below:

/usr/sbin/sntpd 1740 faf

CCI: CCI-001891

Group ID (Vulid): V-223776
Group Title: OS000200
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000200
Rule Title: IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM properly coded.

Vulnerability Discussion: Inaccurate time stamps make it more difficult to
correlate events and can lead to an inaccurate analysis. Determining the correct
time a particular event occurred on a system is critical when conducting
forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time
stamps for information systems with multiple system clocks and systems connected
over a network. Organizations should consider setting time periods for different
types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to
the authoritative time server (e.g., mobile, teleworking, and tactical
endpoints). This requirement is related to the comparison done every 24 hours in
SRG-OS-000355 because a comparison must be done in order to determine the time
difference.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Refer to the CLOCKxx member of PARMLIB.

If the ACCURACY parm is not coded, this is a finding.

If the ACCURACY parm is coded to "1000", this is not a finding.

Fix Text:
Define the CLOCKxx statement to include the ACCURACY parm set to "1000".

CCI: CCI-002046

Group ID (Vulid): V-223777
Group Title: OS000210
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000210
Rule Title: IBM RACF must define UACC of NONE on all profiles.

Vulnerability Discussion: The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Responsibility: Systems Administrator
IAControls: N/A

Check Content:
a) Using Vanguard Administrator select Security Server Reports
b) select Option 3 Data Set Profile
c) Hit ENTER
d) SORT UACC

Review all Dataset and resource profiles in the RACF database.

If any are not defined with UACC NONE, this is a finding.

Fix Text:
Define each dataset and resource profile with UACC(NONE)

CCI: CCI-001774

Group ID (Vulid): V-223778

Group Title: OS000220
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000220
Rule Title: PASSWORD data set and OS passwords are utilized.

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

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

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

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

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

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

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

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

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223780
Group Title: OS000240
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000240
Rule Title: The IBM z/OS Policy Agent must employ a deny-all, allow-by-exception
firewall policy for allowing connections to other systems.

Vulnerability Discussion: Failure to restrict network connectivity only to
authorized systems permits inbound connections from malicious systems. It also
permits outbound connections that may facilitate exfiltration of DoD data.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Examine the policy agent policy statements.

If it can be determined that the policy agent employs a deny-all, allow-by
exception firewall policy for allowing connections to other systems this is not
a finding.

Fix Text:
Develop a policy application and policy agent to employ a deny-all,
allow-by-exception firewall policy for allowing connections to other
systems.

CCI: CCI-000366

CCI: CCI-002080

Group ID (Vulid): V-223781
Group Title: OS000250
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): OS000250
Rule Title: Unsupported system software is installed and active on the
system.

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

Responsibility: N/A
IAControls: N/A

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

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

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

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

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

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

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

CCI: CCI-001764

CCI: CCI-001765

Group ID (Vulid): V-223782
Group Title: OS000260
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): OS000260
Rule Title: Non-existent or inaccessible LINKLIST libraries.

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

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1

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

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

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

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

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

The Linklist is a default set of libraries that MVS searches for a specified

program. This facility is used so that a user does not have to know the library
names in which utility types of programs are stored. Control over membership in
the Linklist is specified within the operating system. The data set
SYS1.PARMLIB(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-223783
Group Title: OS000270
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): OS000270
Rule Title: Non-existent or inaccessible Link Pack Area (LPA) libraries.

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

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1

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

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

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

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

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

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

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

- LPALSTxx specifies the names of libraries to be concatenated to SYS1.LPALIB when the LPA is generated at IPL in an MVS/XA or MVS/ESA system. (The xx is the suffix designated by the LPA parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at system initial program load [IPL].)

- IEAFIXxx specifies the names of modules from SYS1.SVCLIB, the LPALSTxx concatenation, and the LNKLSTxx concatenation that are to be temporarily fixed

in central storage in the Fixed LPA (FLPA) for the duration of an IPL. (The xx
is the suffix designated by the FIX parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at IPL.)

- IEALPAxx specifies the names of modules that will be loaded from the
following:

? SYS1.SVCLIB
? The LPALSTxx concatenation
? The LNKLSTxx concatenation as a temporary extension to the existing
Pageable

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

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

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

CCI: CCI-001762

CCI: CCI-001764

Group ID (Vulid): V-223784
Group Title: OS000280
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): OS000280
Rule Title: Inaccessible APF libraries defined.

Vulnerability Discussion: If a library designated by an APF entry does not
exist on the volume specified, a library of the same name may be placed on this
volume and inherit APF authorization. This could allow the introduction of

modules which bypass security and violate the integrity of the operating system
environment.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:
a) From Analyzer main Menu, go to 4;B. Specify S next to APF table in the upper
half of the screen. Specify YES for Exceptions Only and NO for all other options on the lower half of the screen. Submit the batch job and reference the
report output.

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

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

Fix Text: The systems programmer will ensure that only existing libraries are
specified in the APF list of libraries. Review the entire list of APF authorized
libraries and remove those which are no longer valid designations.
(2) The IEAAPFxx members will contain only required libraries. On a semi annual
basis, Software Support should review the volume serial numbers, and should
verify them in accordance with the system catalog. Software Support will remove
all non existent libraries. The IAO should modify and/or delete the rules associated with these libraries.

CCI: CCI-000381

CCI: CCI-001762

CCI: CCI-002283

Group ID (Vulid): V-223785
Group Title: OS000290
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000290

Rule Title: Inapplicable PPT entries have not been invalidated.

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

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

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

b) Review report for any entries with message VSA334R .

1. If any of the entries in the report that have message VSA334R associated with them have any of the following settings, then there is a FINDING:
a. Bypass password protection: Yes
b. No Dataset Integrity? Yes
c. Protect Key (if required): 00-07

2. If ALL of the entries in the report that have message VSA334R associated with them DO NOT have any of the following settings, then there is NO FINDING:
a. Bypass password protection: Yes
b. No Dataset Integrity? Yes
c. Protect Key (if required): 00-07

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

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

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

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

(1) As part of standard MVS maintenance, systems programming personnel will review the IEFSDPPT module and all programs that IBM has, by default, placed in the PPT to validate their applicability to the execution system. Please refer to the IBM z/OS MVS Initialization and Tuning Reference documentation for the version and release of z/OS installed at the individual site for the actual contents of the default IEFSDPPT

(2) Modules for products not in use on the system will have their special privileges explicitly revoked. Do this by placing a PPT entry for each module in the SYS1.PARMLIB(SCHEDxx) member, specifying no special privileges. The PPT entry for each overridden program will be in the following format, accepting the default (unprivileged) values for the sub parameters:

```
PPT       PGMNAME(<program name>)
```

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

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

CCI: CCI-000381

Group ID (Vulid): V-223786
Group Title: OS000300
Rule ID: N/A

Severity: CAT II
Rule Version (STIG-ID): OS000300
Rule Title: Site must have a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support.

Vulnerability Discussion: Vendors' code may contain vulnerabilities that may be exploited to cause denial of service or to violate the integrity of the system or data on the System. Most vendors develop patches to correct these vulnerabilities. When vendors' products become unsupported, the creation of these patches cease leaving the system exposed to any future vulnerabilities not patched. Without a documented migration plan established to monitor system software versions and releases unsupported software may be allowed to run on the system.

Responsibility: Security Manager
IAControls: N/A

Check Content:
a) Check with the Systems programmer to make sure that documented procedures exist to monitor the software products in SS0 Supported Software Version Release Table in the z/OS STIG Addendum. to verify dates it will become unsupported and to notify management to start procedures to upgrade to supported versions of the products before that date.

b) If documented procedures exist to monitor products in SS0 Supported Software Version Release Table in the z/OS STIG Addendum for dates they will become unsupported and to notify management to upgrade to supported versions of the products this is not a finding.

c) If documented procedures do not exist to monitor products in SS0 Supported Software Version Release Table in the z/OS STIG Addendum for dates they will become unsupported and to notify management to upgrade to supported versions of the products this is a finding.

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

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

CCI: CCI-000409

CCI: CCI-001225

CCI: CCI-001227

CCI: CCI-002606

CCI: CCI-002615

CCI: CCI-002617

Group ID (Vulid): V-223787
Group Title: OS000310
Rule ID: N/A
Severity: CAT III
Rule Version (STIG-ID): OS000310
Rule Title: Duplicated sensitive utilities and/or programs exist in APF libraries.

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

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

Check Content:
a) From Analyzer main Menu, go to 4;B. Specify S next to APF tables in the
upper half of the screen. Specify YES for Duplicate Module Analysis and NO

for all other options on the lower half of the screen. Submit the batch job and
reference the report output. Review the Duplicate Module Analysis section of the
report.

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

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

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

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

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

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

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

CCI: CCI-001762

CCI: CCI-002283

Group ID (Vulid): V-223788
Group Title: OS000320
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000320
Rule Title: The IBM z/OS systems requiring data at rest protection must properly employ IBM DS8880 for full disk encryption for classified systems.

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Determine if IBM's DS880 Disks are in use.

If they are not in use for systems that require data at rest, this is a finding.

Fix Text:
Employ IBM's DS8880 hardware to ensure full disk encryption.

CCI: CCI-002450

Group ID (Vulid): V-223789
Group Title: OS000330
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000330
Rule Title: The IBM z/OS systems requiring data-at-rest protection must properly
employ IBM DS8880 for full disk encryption.

Vulnerability Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive
and tape drive, when used for backups) within an operating system.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Determine if IBM's DS880 Disks are in use.

If they are not in use for systems that require data at rest, this is a finding.

Fix Text:
Employ IBM's DS8880 hardware to ensure full disk encryption.

CCI: CCI-001199

Group ID (Vulid): V-223790
Group Title: OS000340
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000340

Rule Title: IBM z/OS must implement cryptographic mechanisms to prevent unauthorized modification of all information at rest on all operating system
components.

Vulnerability Discussion: Operating systems handling data requiring data at
rest protections must employ cryptographic mechanisms to prevent unauthorized
disclosure and modification of the information at rest.

Satisfies: SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Determine if IBM's DS880 Disks are in use.

If they are not in use for systems that require data at rest, this is a finding.

Fix Text:
Employ IBM's DS8880 hardware to ensure full disk encryption.

CCI: CCI-002475

CCI: CCI-002476

Group ID (Vulid): V-223791
Group Title: OS000350
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000350
Rule Title: Sensitive and critical system data sets exist on shared DASD.

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

the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-2, DCSL-1, ECAN-1, ECCD-1, ECCD-2

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

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

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

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

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

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

HMC
VM
z/OS

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

The IAO will review all access requirements to validate that sensitive and

critical system data sets are protected from unauthorized access across all
systems that have access to the shared volume(s). Protecting the data set(s)
whether the data set(s) are used or not used on the systems that have the shared
volume(s) available to them.

CCI: CCI-000099

CCI: CCI-001090

CCI: CCI-001414

Group ID (Vulid): V-223792
Group Title: OS000360
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000360
Rule Title: The IBM z/OS Policy Agent must contain a policy that protects
against or limits the effects of denial-of-service (DoS) attacks by ensuring the
operating system is implementing rate-limiting measures o

Vulnerability Discussion: DoS is a condition when a resource is not available
for legitimate users. When this occurs, the organization either cannot
accomplish its mission or must operate at degraded capacity.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Examine the Policy Agent policy statements.

If it can be determined that policy that protects against or limits the effects
of denial-of-service (DoS) attacks by ensuring the operating system is
implementing rate-limiting measures on impacted network interfaces, this is not
a finding.

Fix Text:
Develop Policy application and policy agent to protect against or limit the
effects of denial-of-service (DoS) attacks by ensuring the operating system is
implementing rate-limiting measures on impacted network interfaces.

CCI: CCI-002385

Group ID (Vulid): V-223793
Group Title: OS000370
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000370
Rule Title: The IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks.

Vulnerability Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Examine the Policy Agent policy statements.

If it can be determined that there are policy statements that manages excess capacity, this is not a finding.

Fix Text:
Develop Policy application and Policy agent to manage excess capacity.

CCI: CCI-001095

Group ID (Vulid): V-223794
Group Title: OS000400
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000400
Rule Title: The IBM z/OS must employ a session manager that conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Vulnerability Discussion: A session lock is a temporary action taken when a
user stops work and moves away from the immediate physical vicinity of the
information system but does not log out because of the temporary nature of the
absence.

The session lock is implemented at the point where session activity can be
determined. The operating system session lock event must include an obfuscation
of the display screen so as to prevent other users from reading what was
previously displayed.

Publicly viewable images can include static or dynamic images, for example,
patterns used with screen savers, photographic images, solid colors, a clock, a
battery life indicator, or a blank screen, with the additional caveat that none
of the images convey sensitive information.

Responsibility: Systems Prorammer
IAControls: n/a

Check Content:

Ask the system administrator for the configuration parameters for the session
manager in use.

If there is no session manager in use, this is a finding.

If the session manager is not configure to conceal, via the session lock,
information previously visible on the display with a publicly viewable image,
this is a finding.

Fix Text:
Configure the session manager to conceal, via the session lock, information
previously visible on the display with a publicly viewable image.

CCI: CCI-000060

Group ID (Vulid): V-223795
Group Title: OS000410
Rule ID: N/A
Severity: CAT II

Rule Version (STIG-ID): OS000410
Rule Title: IBM z/OS must employ a session manager to manage session lock after
a 15-minute period of inactivity.

Vulnerability Discussion: A session time-out lock is a temporary action taken
when a user stops work and moves away from the immediate physical vicinity of
the information system but does not log out because of the temporary nature of
the absence. Rather than relying on the user to manually lock their operating
system session prior to vacating the vicinity, operating systems need to be able
to identify when a user's session has idled and take action to initiate the
session lock.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Ask the system administrator for the configuration parameters for the session
manager in use.

If there is no session manager in use, this is a finding.

If the session manager is not configured to initiate session lock after a
15-minute period of inactivity, this is a finding.

Fix Text:
Configure the session manager to initiate a session lock after a 15-minute
period of inactivity.

CCI: CCI-000057

Group ID (Vulid): V-223796
Group Title: OS000420
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000420
Rule Title: IBM z/OS must employ a session for users to directly initiate a
session lock for all connection types.

Vulnerability Discussion: The session lock is implemented at the point where
session activity can be determined. Rather than be forced to wait for a period
of time to expire before the user session can be locked, operating systems need
to provide users with the ability to manually invoke a session lock so users may
secure their session should the need arise for them to temporarily vacate the
immediate physical vicinity.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the configuration parameters for the session
manager in use.

If there is no session manager in use, this is a finding.

If the session manager in use does not allow users to directly initiate a
session lock for all connection types, this is a finding.

Fix Text:
Develop a procedure to offload SMF files to a different system or media than the
system being audited.

CCI: CCI-000058

Group ID (Vulid): V-223797
Group Title: OS000430
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000430
Rule Title: IBM z/OS must employ a session manager to manage retaining a users
session lock until that user reestablishes access using established
identification and authentication procedures.

Vulnerability Discussion: A session lock is a temporary action taken when a
user stops work and moves away from the immediate physical vicinity of the
information system but does not want to log out because of the temporary nature
of the absence.

The session lock is implemented at the point where session activity can be
determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates.
No other activity aside from reauthentication must unlock the system.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the configuration parameters for the session
manager in use.

If there is no session manager in use this is a finding.

If the session manager is not configured to retain a user's session lock until
that user reestablishes access using established identification and authentication procedures, this is a finding.

Fix Text:
Configure the session manager to retain a user's session lock until that user
reestablishes access using established identification and authentication procedures.

CCI: CCI-000056

Group ID (Vulid): V-223798
Group Title: OS000440
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000440
Rule Title: IBM z/OS system administrator must develop a procedure to remove or
disable temporary user accounts after 72 hours.

Vulnerability Discussion: Emergency accounts are privileged accounts that are
established in response to crisis situations where the need for rapid account
activation is required. Therefore, emergency account activation may bypass

normal account authorization processes. If these accounts are automatically
disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to automatically remove or disable temporary user accounts after 72 hours.

If there is no procedure, this is a finding.

Fix Text:
Develop a procedure to automatically remove or disable temporary user accounts
after 72 hours.

CCI: CCI-000016

Group ID (Vulid): V-223799
Group Title: OS000450
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000450
Rule Title: IBM z/OS system administrator must develop a procedure to remove or
disable emergency accounts after the crisis is resolved or 72 hours.

Vulnerability Discussion: IBM z/OS system administrator must develop a procedure to remove or disable emergency accounts after the crisis is resolved
or 72 hours.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to automatically remove or disable emergency accounts after the crisis is resolved or 72 hours.

If there is no procedure, this is a finding.

Fix Text:

Develop a procedure to remove or disable emergency user accounts after the
crisis is resolved or 72 hours.

CCI: CCI-001682

Group ID (Vulid): V-223800
Group Title: OS000460
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000460
Rule Title: IBM z/OS system administrator must develop a procedure to notify
designated personnel if baseline configurations are changed in an unauthorized
manner.

Vulnerability Discussion: Unauthorized changes to the baseline configuration
could make the system vulnerable to various attacks or allow unauthorized access
to the operating system. Changes to operating system configurations can have
unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid
unintended, negative consequences that could ultimately affect the security
state of the operating system. The operating system's IMO/ISSO and SAs must be
notified via email and/or monitoring system trap when there is an unauthorized
modification of a configuration item.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to notify designated personnel if
baseline configurations are changed in an unauthorized manner.

If there is no procedure, this is a finding.

Fix Text:
Develop a procedure to notify designated personnel if baseline configurations
are changed in an unauthorized manner.

CCI: CCI-001744

Group ID (Vulid): V-223801
Group Title: OS000470
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000470
Rule Title: IBM z/OS system administrator must develop a procedure to provide an audit reduction capability that supports on-demand reporting requirements.

Vulnerability Discussion: If a maintenance session or connection remains open after maintenance is completed, it may be hijacked by an attacker and used to compromise or damage the system.

Some maintenance and test tools are either standalone devices with their own operating systems or are applications bundled with an operating system.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to provide an audit reduction capability that supports on-demand reporting requirements.

If there is no procedure, this is a finding.

Fix Text:
Develop a procedure to provide an audit reduction capability that supports on-demand reporting requirements.

CCI: CCI-001876

Group ID (Vulid): V-223802
Group Title: OS000480
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000480
Rule Title: IBM z/OS system administrator must develop a procedure to terminate all sessions and network connections related to nonlocal maintenance when nonlocal maintenance is completed.

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to terminate all sessions and network connections related to nonlocal maintenance when nonlocal maintenance is completed.

If there is no procedure, this is a finding.

Fix Text:
Develop a procedure to terminate all sessions and network connections related to nonlocal maintenance when nonlocal maintenance is completed.

CCI: CCI-000879

Group ID (Vulid): V-223803
Group Title: OS000490
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000490
Rule Title: IBM z/OS system administrator must develop a procedure to remove all software components after updated versions have been installed.

Vulnerability Discussion: Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to remove all software components after updated versions have been installed.

If there is no procedure, this is a finding.

Fix Text:
Develop a procedure to remove all software components after updated versions have been installed.

CCI: CCI-002617

Group ID (Vulid): V-223804
Group Title: OS000500
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000500
Rule Title: IBM z/OS must shut down the information system, restart the information system, and/or notify the system administrator when anomalies in the operation of any security functions are discovered.

Vulnerability Discussion: If anomalies are not acted upon, security functions may fail to secure the system.

Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Notifications provided by information systems include messages to local computer consoles, and/or hardware indications, such as lights.

This capability must take into account operational requirements for availability for selecting an appropriate response. The organization may choose to shut down or restart the information system upon security function anomaly detection.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies occur.

If a procedure does not exist, this is a finding.

If the procedure does not properly shut down the information system, restart the information system, and/or notify the system administrator when anomalies occur, this is a finding.

Fix Text:
Develop a procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies occur.

CCI: CCI-002702

Group ID (Vulid): V-223805
Group Title: OS000510
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): OS000510
Rule Title: IBM z/OS system administrator must develop a procedure to offload
SMF files to a different system or media than the system being audited.

Vulnerability Discussion: Information stored in one location is vulnerable to
accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Responsibility: System Administrator
IAControls: N/A

Check Content:

Ask the system administrator for the procedure to offload SMF files to a different system or media than the system being audited.

If the procedure does not exist, this is a finding.

Fix Text:
Develop a procedure to offload SMF files to a different system or media than the
system being audited.

CCI: CCI-001851

Group ID (Vulid): V-223806
Group Title: SH000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SH000010
Rule Title: SMF recording options for the SSH daemon must be configured to write
SMF records for all eligible events.

Vulnerability Discussion: SMF data collection is the basic unit of tracking of
all system functions and actions. Included in this tracking data are the audit

trails from each of the ACPs. If the control options for the recording of this
tracking are not properly maintained, then accountability cannot be monitored,
and its use in the execution of a contingency plan could be compromised.

Responsibility: N/A
IAControls: N/A

Check Content:
a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager,
then Option 2; Unix File Manager.

b) Locate the SSH daemon configuration file. This file may be found in the
/etc/ssh/ directory.

c) If SSH Daemon is not active, there is NO FINDING.

d) Examine SSH daemon configuration file.

1. If Server SMF is not coded with ServerSMF TYPE119_U83, this is a FINDING.
2. If Server SMF is commented out, this is a FINDING

Fix Text: Configure the SERVERSMF statement in the SSH Daemon configuration file
to TYPE119_U83.

Group ID (Vulid): V-223807
Group Title: SH000020
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): SH000020
Rule Title: The SSH daemon must be configured to use a FIPS 140-2 compliant
cryptographic algorithm.

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. Cryptographic
modules must adhere to the higher standards approved by the federal government
since this provides assurance they have been tested and validated.

Responsibility: N/A
IAControls: N/A

Check Content:

a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager,
then Option 2; Unix File Manager.

b) Locate the SSH daemon configuration file. This file may be found in the
/etc/ssh/ directory.

c) Examine SSH daemon configuration file sshd_config.

1. If there are no Ciphers lines or the ciphers list contains any cipher
not starting with 3des or aes, this is a FINDING.
2. If the Macs line is not configured to hmac-shal or greater, this is a
FINDING.

d) Examine the z/OS-specified sshd server system-wide configuration zos_sshd_config.

1. If any of the following is untrue, this is a FINDING.
i. FTPSMODE YES
ii. CipherSource ICSF
iii. MACsSource ICSF

Fix Text: Edit the SSH daemon configuration and remove any ciphers not starting
with "3des" or "aes". If necessary, add a "Ciphers" line using FIPS 140-2 compliant algorithms.

Configure for message authentication to MACs "hmac-sha1" or greater.

Edit the z/OS-specific sshd server system-wide configuration file configuration
as follows:
FIPSMODE YES
CiphersSource ICSF
MACsSource ICSF

Group ID (Vulid): V-223808
Group Title: SH000030
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): SH000030
Rule Title: The IBM z/OS must implement DoD-approved encryption to protect the
confidentiality of remote access sessions.

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. Cryptographic

modules must adhere to the higher standards approved by the federal government
since this provides assurance they have been tested and validated.

Responsibility: N/A
IAControls: N/A

Check Content:

a) Locate the SSH daemon configuration file, which may be found in /etc/ssh/
directory.

b) 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

Generic profiles and commands should also be enabled with the command SETR
GENERIC(SERVAUTH) GENCMD(SERVAUTH).

CCI: CCI

CCI: CCI-001453

Group ID (Vulid): V-223809
Group Title: SH000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SH000040
Rule Title: The SSH daemon must be configured with the Department of Defense
(DoD) logon banner.

Vulnerability Discussion: Failure to display the DoD logon banner prior to a
logon attempt will negate legal proceedings resulting from unauthorized access
to system resources.

Responsibility: N/A
IAControls: N/A

Check Content:
a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager,
then Option 2; Unix File Manager.

b) Locate the SSH daemon configuration file. This file may be found in the
/etc/ssh/ directory.

c) If SSH Daemon is not active, there is NO FINDING.

d) Examine SSH daemon configuration file.

1. If Banner statement is missing or configured to none, this is a FINDING.
2. Ensure that the contents of the file specified on the banner statement
contain a logon banner. The below banner is mandatory and deviations are not
permitted except as authorized in writing by the DoD Chief Information Officer.
If there is any deviation, this is a FINDING.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement (LE),
and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services
by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement
for details.

Fix Text: Configure the banner statement to a file that contains the Department
of Defense (DoD) logon banner.

Ensure that the contents of the file specified on the banner statement contain a
logon banner.
The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

-The USG routinely intercepts and monitors communications on this IS for

purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement (LE),
and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or services
by attorneys, psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See User Agreement
for details.

Group ID (Vulid): V-223810
Group Title: SH000050
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): SH000050
Rule Title: The SSH daemon must be configured to only use the SSHv2 protocol.

Vulnerability Discussion: SSHv1 is not a DoD-approved protocol and has many
well-known vulnerability exploits. Exploits of the SSH daemon could provide
immediate root access to the system.

Responsibility: N/A
IAControls: N/A

Check Content:
a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager,
then Option 2; Unix File Manager.

b) Locate the SSH daemon configuration file. This file may be found in the

/etc/ssh/ directory.

c) If SSH Daemon is not active, there is NOFINDING.

d) Examine SSH daemon configuration file.

1. If variable 'Protocol 2' is defined, there is NO FINDING.
2. If variable 'Protocol' is defined in a leading comment or has a value
other than 2, this is a FINDING.

Fix Text: Edit the sshd_config file and set the "Protocol" setting to "2".

Group ID (Vulid): V-223811
Group Title: SH000060
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SH000060
Rule Title: IBM z/OS, for PKI-based authentication, must use the ESM for key
management.

Vulnerability Discussion: Without mapping the certificate used to authenticate
to the user account, the ability to determine the identity of the individual
user or group will not be available for forensic analysis.

Responsibility: N/A
IAControls: N/A

Check Content:

From the ISPF Command Shell enter:
OMVS
enter
find / -name *.kdb
find / -name *.jks
If any files are found, this is a finding

Fix Text:
Define all Keys/Certificates to the security database.

Remove the all .kdb files.

CCI: CCI-000187

Group ID (Vulid): V-223812
Group Title: SL000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SL000010
Rule Title: The permission bits and user audit bits for HFS objects that are
part of the Syslog daemon component will be configured properly.

Vulnerability Discussion: HFS directories and files of the Syslog daemon provide the configuration and executable properties of this product. Failure to
properly secure these objects could lead to unauthorized access. This exposure
may result in the compromise of the integrity and availability of the operating
system environment, ACP, and customer data.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
permission
bits and user audit bits for HFS objects that are part of the Syslog daemon
component are
configured according to the settings in the following table:

SYSLOG DAEMON HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION BITS	USERAUDIT BITS
/usr/sbin/syslogd	1740	fff
/etc/syslog.conf	0744	faf
[Output log file defined in the configuration file]	0744	fff

a) Using Vanguard Administrator UNIX file manager option 14 review the files
listed in the table above.

b) If the HFS permission bits and user audit bits for each directory and file
match or
are more restrictive than the specified settings listed in this table, there is
NO
FINDING.

NOTES:
The /usr/sbin/syslogd object is a symbolic link to
/usr/lpp/tcpip/sbin/syslogd.
The
permission and user audit bits on the target of the symbolic link must
have the
required settings.

The /etc/syslog.conf file may not be the configuration file the daemon
uses. It
is
necessary to check the script or JCL used to start the daemon to
determine the
actual configuration file.

For example, in /etc/rc:
 _BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf

 For example, in the SYSLOGD started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f //''SYS1.TCPPARMS(SYSLOG)'''
```

 The following represents a hierarchy for permission bits from least
restrictive
to most
restrictive:

7 rwx(least restrictive)
6 rw
3 -wx
2 w-
5 r-x
4 r--
1--x
0 ---(most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
-no auditing

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

Fix Text: The IAO with the assistance of a systems programmer with UID(0)
and/or
SUPERUSER access, will review the UNIX permission bits and user audit
bits on

the HFS directories and files for the Syslog daemon. Ensure they conform to the
specifications in the SYSLOG Daemon HFS Object Security Settings table below.

Log files should have security that prevents anyone except the syslogd process
and authorized maintenance jobs from writing to or deleting them.

A maintenance process to periodically clear the log files is essential. Logging
stops if the target file system becomes full.

SYSLOG Daemon HFS Object Security Settings

File	Permission Bits	User Audit Bits
/usr/sbin/syslogd	1740	fff
[Configuration File]		
/etc/syslog.conf	0744	faf
[Output log file defined in the configuration file]		
	0744	fff

The following represents a hierarchy for permission bits from least restrictive
to most restrictive:

7	rwx	(least restrictive)
6	rw-	
3	-wx	
2	-w-	
5	r-x	
4	r--	
1	--x	
0	---	(most restrictive)

The possible audit bits settings are as follows:

f	log for failed access attempts
a	log for failed and successful access
-	no auditing

NOTES:
The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd.
The permission and user audit bits on the target of the symbolic link must have
the required settings.

The /etc/syslog.conf file may not be the configuration file the daemon uses. It
is necessary to check the script or JCL used to start the daemon to determine
the actual configuration file. For example, in /etc/rc:

```
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf
```

For example, in the SYSLOGD started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f //''SYS1.TCPPARMS(SYSLOG)'''
```

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/syslogd
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd
chmod 0744 /etc/syslog.conf
chaudit w=sf,rx+f /etc/syslog.conf
chmod 0744 /log_dir/log_file
chaudit rwx=f /log_dir/log_file
```

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-223813
Group Title: SL000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SL000020
Rule Title: The Syslog daemon is not started at z/OS initialization.

Vulnerability Discussion: The Syslog daemon, known as SYSLOGD, is a z/OS UNIX daemon that provides a central processing point for log messages issued by other z/OS UNIX processes. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. It is important that SYSLOGD be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that Syslogd
is
started at Z/OS system initialization.

NOTE: Syslogd may be started from the shell, a cataloged procedure (STC), or the
BPXBATCH program. Additionally, other mechanisms (e.g., CONTROL-O) may be used to automatically start the Syslog daemon. To thoroughly analyze this PDI
you may
need to view the OS SYSLOG using SDSF, find the last IPL, and look for the
initialization of Syslogd.

a) If the Syslog daemon Syslogd is started automatically during the initialization of
the z/OS system, there is NO FINDING.

b) If (a) is untrue, this is a FINDING.

Fix Text: Review the files used to initialize tasks during system IPL (e.g.,
/etc/rc, SYS1.PARMLIB, CONTROL-O definitions) to ensure the Syslog daemon is
automatically started during z/OS system initialization.

It is important that syslogd be started during the initialization phase of the
z/OS system to ensure that significant messages are not lost. As with other z/OS
UNIX daemons, there is more than one way to start SYSLOGD. It can be started as
a process in the /etc/rc file or as a z/OS started task.

CCI: CCI-000764

CCI: CCI-002234

Group ID (Vulid): V-223814
Group Title: SL000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SL000030
Rule Title: The Syslog daemon must be properly defined and secured.

Vulnerability Discussion: The Syslog daemon, known as syslogd, is a zOS UNIX daemon that provides a central processing point for log messages issued by other zOS UNIX processes. It is also possible to receive log messages from other network-connected hosts. Some of the IBM Communications Server components that may send messages to syslog are the FTP, TFTP, zOS UNIX Telnet, DNS, and DHCP servers. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. Primarily because of the potential to use this information in an audit process, there is a security interest in protecting the syslogd process and its associated data.

The Syslog daemon requires special privileges and access to sensitive resources to provide its system services. Failure to properly define and control the Syslog daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:
The systems programmer responsible for supporting ICS will ensure that Syslogd runs under its own user account. Specifically, it does not share the account defined for the Z/OS UNIX kernel.

The systems programmer responsible for supporting ICS will ensure that Syslogd runs with a job/started task name such as SYSLOGD that uniquely identifies it.
1) If you start SYSLOGD from MVS then ensure the following:
a) The SYSLOG daemon userid is SYSLOGD.
b) The SYSLOGD userid is defined as a PROTECTED userid.
c) The SYSLOGD userid has the following z/OS OMVS attributes: UID(0) HOME(/) PROGRAM(/bin/sh)
d) A matching entry in the STARTED class exists mapping the SYSLOGD started proc to the SYSLOGD userid.

To do the above:
Display the active started tasks executing on the domain using SDSF, or

equivalent JES display product, and locate the SYSLOGD started task. Document the USERID.

Using Vanguard Administrator User Profile summery mask on USERID = syslogd userid. Use the LV command and review the USERID and ensure all items are in effect for the Syslog daemon:

2) If you start SYSLOGD from /etc/rc then ensure the following:
a) The _BPX_JOBNAME environment variable is set to assign a job name of SYSLOGD.

To do the above:
 You will need to locate the /etc/rc file and locate the BPX_JOBNAME in it.

c) If SYSLOGD is started from MVS then if b(1) is true, there is NO FINDING.

d) If SYSLOGD is started from within USS then if b(2) is true, there is NO
FINDING.

e) If SYSLOGD is started from within MVS and b(1) is untrue, this is a FINDING.

f) If SYSLOGD is started from within USS and b(2) is untrue, this is a FINDING.

Fix Text: The IAO working with the systems programmer responsible for supporting
IBM Comm Server will ensure that Syslog daemon runs under its own user account.
Specifically, it does not share the account defined for the z/OS UNIX kernel.

The Syslog daemon userid is SYSLOGD.
The SYSLOGD userid is defined as a PROTECTED userid.
The SYSLOGD userid has UID(0), HOME(/), and PROGRAM(/bin/sh) specified in
the OMVS segment.

To set up and use as an MVS Started Proc, the following sample commands are
provided:

```
AU SYSLOGD NAME('stc, tcpip') NOPASSWORD NOOIDCARD DFLTGRP(STC)
OWNER(STC) DATA('Reference ISLG0020 for proper setup ')
ALU SYSLOGD DFLTGRP(stctcpx)
ALU SYSLOGD OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))
CO SYSLOGD GROUP(stctcpx) OWNER(stctcpx)
```

A matching entry mapping the SYSLOGD started proc to the SYSLOGD userid is in

the STARTED resource class.

RDEF STARTED SYSLOGD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
STDATA(USER(SYSLOGD) GROUP(STC))

If /etc/rc is used to start the Syslog daemon ensure that the
_BPX_JOBNAME and
BPX USERID environment variables are assigned a value of SYSLOGD.

CCI: CCI-000764

Group ID (Vulid): V-223815
Group Title: SM000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SM000010
Rule Title: IBM z/OS DFSMS Program Resources must be properly defined and protected.

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be
properly configured to incorporate access control methods that do not rely
solely on the possession of a certificate for access. Successful authentication
must not automatically give an entity access to an asset or security boundary.
Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use
access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies,
and attribute-based policies. Access enforcement mechanisms include: access
control lists, access control matrices, and cryptography. These policies and
mechanisms must be employed by the application to control access between users
(or processes acting on behalf of users) and objects (e.g., devices, files,
records, processes, programs, and domains) in the information system.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:

Refer to the load modules residing in the following Load libraries to determine
program resource definitions:
 SYS1.DGTLLIB for DFSMSdfp/ISMF
 SYS1.DGTLLIB for DFSMSdss/ISMF
 SYS1.DFQLLIB for DFSMShsm

If the installation moves these modules to another load library the installation-defined load library must be used in the program protection.

If the RACF resources are defined with a default access of NONE, this is not a
finding.

If the RACF resource access authorizations restrict access to the appropriate
personnel, this is not a finding.

(Refer to the chapter titled Protecting the Storage Management Subsystem in the
IBM z/OS DFSMSdfp Storage Administration Guide to assist with guidance on appropriate access.)

Fix Text:
(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.)

Refer to the chapter titled Protecting the Storage Management Subsystem in the
IBM z/OS DFSMSdfp Storage Administration Guide.

Use SMS Program Resources tables to determine the resources and access requirements for SMS Program Resources. Ensure the guidelines for the resource
type, resources, and/or generic equivalent are specified.

The RACF resources as designated in the table above are defined with a default
access of NONE.

The RACF resource access authorizations restrict access to the appropriate
personnel as designated in the table above.

The following commands are provided as a sample for implementing resource controls:

```
RDEF PROGRAM ACBFUTO2 ADDMEM('SYS1.DSF.DGTLLIB'//NOPADCHK) -
DATA('ADDED PER SRR PDI ZSMS0012 ') -
AUDIT(FAILURE(READ)) UACC(NONE) OWNER(ADMIN)
PERMIT ACBFUTO2 CLASS(PROGRAM) ID(********)
```

CCI: CCI-000213

Group ID (Vulid): V-223816
Group Title: SM000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SM000020
Rule Title: DFSMS control data sets are not protected in accordance with security requirements.

Vulnerability Discussion: DFSMS control data sets provide the configuration and operational characteristics of the system-managed storage environment. Failure to properly protect these data sets may result in unauthorized access. This exposure could compromise the availability and integrity of some system services and customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Refer to the following item gathered from the Data Facility Storage Management Subsystem (DFSMS) Worksheet in the Preliminary Information Worksheets in U_zOS_STIG_INSTRUCTION.doc:

___ 1. Provide the following DFSMS data set names:

SCDS:

ACDS:

COMMDS:

ACS:

ACDS Backup:

COMMDS Backup:

b) Generate a report for security verification using Analyzer.
1. Select option 4 Batch Reports from the Analyzer main menu
2. Select option B Sensitive and Critical Data Sets Analysis
3. Enter R on line item User defined list
4. Provide a dataset name or your choice which will include the names of the
data sets gathered from step a) above.
 Note: This may be a sequential data set or a PDS member

5. Specify the options as listed here.

AC(1) module list ===NO Duplicate Module Analysis ===NO
RACF detail ===YES Exceptions only ===NO
RACF Group detail ===YES
Search criteria ===NO
Sort criteria ===NO

6. Press enter to invoke the JCL Submit Processing
7. Enter S to submit the batch report
8. Review the report for findings

c) 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

d) If the RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets
restrict UPDATE and ALTER access to only Z/OS systems programming personnel, there is NO FINDING.

e) If the RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets
do not restrict UPDATE and ALTER access to only Z/OS systems programming personnel, this is a FINDING.

Fix Text: b) Review the SYS1.PARMLIB(IGDSMS00) data set to identify the
fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)
Active Control Data Set (ACDS)
Communications Data Set (COMMDS)
Automatic Class Selection Routine Source Data Sets (ACS)
ACDS Backup
COMMDS Backup

The RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets must
restrict UPDATE and ALTER 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.

Some example commands to implement the proper controls are shown here:

```
AD 'sys3.dfsms.mmd.commds.**' UACC(NONE) OWNER(SYS3) AUDIT(ALL(READ))
DATA('PROTECTED PER ZSMS0020')

PE 'sys3.dfsms.mmd.commds.**' ID(<syspaudt>) ACC(A)
```

CCI: CCI-000213

Group ID (Vulid): V-223817
Group Title: SM000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SM000030
Rule Title: DFSMS-related RACF classes are not active.

Vulnerability Discussion: DFSMS provides data, storage, program, and device
management functions for the operating system. Some DFSMS storage administration
functions allow a user to obtain a privileged status and effectively bypass all
ACP data set and volume controls. Failure to properly protect DFSMS resources
may result in unauthorized access. This exposure could compromise the
availability and integrity of the operating system environment, system services,
and customer data.

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

Check Content:
a) Generate a batch report of ACTIVE RACF CLASSES using Analyzer. Review the output.
1. Option 4 Batch Reports, from the Analyzer main menu
2. Option 1: Class Descriptor Table Analysis
3. Submit the job.

b) Verify the following are classes are ACTIVE - MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resources classes.

c) Verify the following classes are RACLISTED - MGMTCLAS and STORCLAS

resource classes.

d) If (b) and (c) are true, there is NO FINDING.

e) If (b) or (c) is not true, this is a FINDING.

Fix Text: CLASSACT Resources

ACTIVE CLASSES lists the MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resources
classes.

The classes can be activated with the command:
SETR CLASSACT(MGMTCLAS STORCLAS PROGRAM FACILITY)

RACLIST CLASSES lists the MGMTCLAS and STORCLAS resource classes.

The classes can be RACLISTED with the command:
SETR RACL(MGMTCLAS STORCLAS)

CCI: CCI-000213

Group ID (Vulid): V-223818
Group Title: SM000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SM000040
Rule Title: DFSMS resources must be protected in accordance with the proper
security requirements.

Vulnerability Discussion: DFSMS provides data, storage, program, and device
management functions for the operating system. Some DFSMS storage administration
functions allow a user to obtain a privileged status and effectively bypass all
ACP data set and volume controls. Failure to properly protect DFSMS resources
may result in unauthorized access. This exposure could compromise the
availability and integrity of the operating system environment, system services,
and customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
a) Generate a report of FACILITY class profiles beginning with STGADMIN, using
the Administrator QUICK GEN utility.

1. Option 3 Security Server Reports from the Administrator main menu.
2. Option 4 General Resource Profile.
3. Under the standard masking fields
Profile: STGADMIN*
Class: FACILITY
4. Enter command option 1
5. At the resulting profile list enter command option QG
6. On line 1 in the edit field enter the following:
 rlist &CLASS (&PROFILE) all
7. On the command line enter GEN
8. Enter VRABATCH. This will submit a batch job. Review the report.

b) Ensure that the following items are in effect:
1. The STGADMIN.** profile in the FACILITY resource class has a default access of NONE and grants no access at this level.
2. STGADMIN.DPDSRN.olddsname is restricted to System Programmers only.
3. The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to System Programmers.
4. The STGADMIN.IGG.DEFDEL.UALIAS is restricted to System Programmers and Security personnel.
5. The STGADMIN.IGG.CATALOG.SECURITY.CHANGE is defined with access of NONE and all access logged

Note: the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE can be defined with read access for migration purposes. If it is a detailed migration plan it 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 = NONE.

NOTE: The following STGADMIN resource profiles may be allocated to the enduser resulting in NO FINDING:

STGADMIN.ADR.COPY.CNCURRNT
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

6. The STGADMIN resource profiles below are restricted to System programmers, DASD managers and Application Production Support Team members. For STGADMIN.IDC.DCOLLECT, Automated Operations can have access also.

STGADMIN.ARC.CANCEL
STGADMIN.ARC.LIST
STGADMIN.ARC.QUERY
STGADMIN.ARC.REPORT

STGADMIN.DMO.CONFIG STGADMIN
STGADMIN.IDC.DCOLLECT
STGADMIN.IFG.READVTOC
STGADMIN.IGG.DELGDG.FORCE

7. STGADMIN resource profiles are controlled using the first two high-leve
resource name qualifiers (as below) at a minimum and restricted to System
programmers and DASD managers.

STGADMIN.ADR
STGADMIN.ANT
STGADMIN.ARC
STGADMIN.DMO
STGADMIN.ICK
STGADMIN.IDC
STGADMIN.IFG
STGADMIN.IGG
STGADMIN.IGWSHCDS

8. The following Storage Administrator functions are controlled using the first three high-level resource name qualifiers at a minimum; restricted to
System programmers and DASD managers and all access is logged.

STGADMIN.ADR.STGADMIN.BUILDSA
STGADMIN.ADR.STGADMIN.COMPRESS
STGADMIN.ADR.STGADMIN.COPY
STGADMIN.ADR.STGADMIN.COPY.DELETE
STGADMIN.ADR.STGADMIN.COPY.RENAME
STGADMIN.ADR.STGADMIN.DEFRAG
STGADMIN.ADR.STGADMIN.DUMP
STGADMIN.ADR.STGADMIN.DUMP.DELETE
STGADMIN.ADR.STGADMIN.PRINT
STGADMIN.ADR.STGADMIN.RELEASE
STGADMIN.ADR.STGADMIN.RESTORE
STGADMIN.ADR.STGADMIN.RESTORE.RENAME

9. All access to the following STGADMIN resources is logged:

STGADMIN.DPDSRN.olddsname
STGADMIN.IGG.DEFDEL.UALIAS
STGADMIN.IGD.ACTIVATE.CONFIGURATION

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

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

Fix Text: The IAO 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.)

Below is listed the access requirements for SMS Resources. Ensure the guidelines
for the resources and/or generic equivalent are followed.

The RACF resources are defined with a default access of NONE.

The RACF resource rules for the resources specify UACC(NONE) and NOWARNING.

Ensure that no access is given to the high-level STGADMIN resource.

Example:

```
RDEF FACILITY STGADMIN.** OWNER(ADMIN) -
UACC(NONE) AUDIT(ALL(READ))
```

Ensure no access is given to resource
STGADMIN.IGG.CATALOG.SECURITY.CHANGE.
Example:

```
RDEF FACILITY STGADMIN.IGG.CATALOG.SECURITY.CHANGE OWNER(ADMIN)
UACC(NONE) AUDIT(ALL(READ))
```

The STGADMIN.DPDSRN.olddsname is restricted to System Programmers and all access
is logged.

Example:

```
RDEF FACILITY STGADMIN.DPDSRN.olddsname OWNER(ADMIN) -
UACC(NONE) AUDIT(ALL(READ))

PE STGADMIN.DPDSRN.olddsname CL(FACILITY) ID(syspaudt)
```

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to System Programmers and
all access is logged.

Example:

```
RDEF FACILITY STGADMIN.IGD.ACTIVATE.CONFIGURATION OWNER(ADMIN) -
UACC(NONE) AUDIT(ALL(READ))

PE STGADMIN.IGD.ACTIVATE.CONFIGURATION CL(FACILITY) ID(syspaudt)
```

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to System Programmers and Security
personnel and all access is logged.

Example:

```
RDEF FACILITY STGADMIN.IGG.DEFDEL.UALIAS OWNER(ADMIN) -
UACC(NONE) AUDIT(ALL(READ))

PE STGADMIN.IGG.DEFDEL.UALIAS CL(FACILITY) ID(secaaudt)
PE STGADMIN.IGG.DEFDEL.UALIAS CL(FACILITY) ID(secdaudt)
PE STGADMIN.IGG.DEFDEL.UALIAS CL(FACILITY) ID(syspaudt)
```

The following resources and prefixes may be available to the end-user.

STGADMIN.ADR.COPY.CNCURRNT
STGADMIN.ADR.COPY.FLASHCPY
STGADMIN.ADR.COPY.TOLERATE.ENQF
STGADMIN.ADR.DUMP.CNCURRNT
STGADMIN.ADR.DUMP.TOLERATE.ENQF
STGADMIN.ADR.RESTORE.TOLERATE.ENQF
STGADMIN.ARC.ENDUSER.
STGADMIN.IGG.ALTER.SMS

Example:

```
RDEF FACILITY STGADMIN.ADR.COPY.CNCURRNT.** OWNER(ADMIN) -
UACC(NONE) AUDIT(FAILURE(READ))

PE STGADMIN.ADR.COPY.CNCURRNT.** CL(FACILITY) ID(endusers)
```

The following resource is restricted to Application Production Support Team
members, Automated Operations, DASD managers, and System programmers.

STGADMIN.IDC.DCOLLECT

Example:

```
RDEF FACILITY STGADMIN.IDC.DCOLLECT.** OWNER(ADMIN) -
UACC(NONE) AUDIT(FAILURE(READ))

PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(appsaudt)
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(autoaudt)
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(dasbaudt)
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(dasdaudt)
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(syspaudt)
```

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:

```
RDEF FACILITY STGADMIN.ARC.CANCEL.** OWNER(ADMIN) -
UACC(NONE) AUDIT(FAILURE(READ))

PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(appsaudt)
PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(dasbaudt)
PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(dasdaudt)
PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(syspaudt)
```

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:

```
RDEF FACILITY STGADMIN.ADR.** OWNER(ADMIN) -
UACC(NONE) AUDIT(FAILURE(READ))

PE STGADMIN.ADR.** CL(FACILITY) ID(dasbaudt)
PE STGADMIN.ADR.** CL(FACILITY) ID(dasdaudt)
PE STGADMIN.ADR.** CL(FACILITY) ID(syspaudt)
```

The following Storage Administrator functions prefix is restricted to DASD
managers and System programmers and all access is logged.

```
STGADMIN.ADR.STGADMIN.
```

Example:

```
RDEF FACILITY STGADMIN.ADR.STGADMIN.** OWNER(ADMIN) -
UACC(NONE) AUDIT(ALL(READ))

PE STGADMIN.ADR.STGADMIN.** CL(FACILITY) ID(dasbaudt)
PE STGADMIN.ADR.STGADMIN.** CL(FACILITY) ID(dasdaudt)
PE STGADMIN.ADR.STGADMIN.** CL(FACILITY) ID(syspaudt)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223819
Group Title: SM000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): SM000050
Rule Title: SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings are not properly specified.

Vulnerability Discussion: Configuration properties of DFSMS are specified in various members of the system parmlib concatenation (e.g., SYS1.PARMLIB). Statements within these PDS members provide the execution, operational, and configuration characteristics of the system-managed storage environment. Missing or inappropriate configuration values may result in undesirable operations and degraded security. This exposure could potentially compromise the availability and integrity of some system services and customer data.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
a) Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), for the following SMS parameter settings:

Parameter Key
SMS
ACDS(ACDS data set name)
COMMDS(COMMDS data set name)

b) If the required parameters are defined, there is NO FINDING.

c) If the required parameters are not defined, this is a FINDING.

Fix Text: The Systems programmer will review the DFSMS-related PDS members and statements specified in the system parmlib concatenation. Ensure these elements are configured as outlined below:

Parameter Key

SMS
ACDS(ACDS data set name)
COMMDS(COMMDS data set name)

CCI: CCI-000366

Group ID (Vulid): V-223820
Group Title: TC000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TC000010
Rule Title: PROFILE.TCPIP configuration statements for the TCP/IP stack are not
coded properly.

Vulnerability Discussion: The PROFILE.TCPIP configuration file provides system
operation and configuration parameters for the TCP/IP stack. Inappropriate
values could result in undesirable operations and degraded security. This
exposure may result in unauthorized access impacting data integrity or the
availability of some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
DELETE
statement is not coded in PROFILE.TCPIP files for production systems.

The systems programmer responsible for supporting ICS will ensure that the
SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT
operands.

The systems programmer responsible for supporting ICS will ensure that the
SMFPARMS statement is not used.

The systems programmer responsible for supporting ICS will ensure that the
TCPCONFIG and UDPCONFIG statements are coded with (at least) the
RESTRICTLOWPORTS operand.

a) Display the active started tasks executing on the domain using SDSF, or
equivalent JES display product, and locate the TCPIP started task. Locate the
TCPIP configuration file identified by the PROFILE DD statement. From the
ISPF Primary Option Menu use option 3.4 and review the TCPIP.DATA
configuration file.

b) Ensure the following items are in effect for the configuration statements
specified
in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

1. The SMFPARMS statement is not coded or commented out.
2. The DELETE statement is not coded or commented out for production
systems.
3. The SMFCONFIG statement is coded with (at least) the FTPCLIENT and
TN3270CLIENT operands.
4. The TCPCONFIG and UDPCONFIG statements are coded with (at least) the
RESTRICTLOWPORTS operand.

Fix Text: Review the configuration statements in the PROFILE.TCPIP file and
ensure they conform to the specifications below:

Ensure the following items are in effect for the configuration statements
specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

1) The SMFPARMS statement is not coded or commented out.
2) The DELETE statement is not coded or commented out for production
systems.
3) The SMFCONFIG statement is coded with (at least) the FTPCLIENT and
TN3270CLIENT operands.
4) The TCPCONFIG and UDPCONFIG statements are coded with (at least) the
RESTRICTLOWPORTS operand.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked

for access authorization compliance in STIG ID ITCP0070.

BASE TCP/IP PROFILE.TCPIP CONFIGURATION STATEMENTS
FUNCTIONS

INCLUDE- Specifies the name of an MVS data set that contains additional PROFILE.TCPIP statements to be used
- It Alters the configuration specified by previous statements

SMFPARMS- Specifies SMF logging options for some TCP applications; replaced by
SMFCONFIG
- Controls collection of audit data

DELETE- Specifies some previous statements, including PORT and PORTRANGE, that
are to be deleted
- Alters the configuration specified by previous statements

SMFCONFIG- - Specifies SMF logging options for Telnet, FTP, TCP, API, and stack
activity
- Controls collection of audit data

TCPCONFIG- Specifies various settings for the TCP protocol layer of TCP/IP
- Controls port access

CCI: CCI-000067

Group ID (Vulid): V-223821
Group Title: TC000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TC000020
Rule Title: IBM z/OS must be configured to restrict all TCP/IP ports to ports,
protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.

Vulnerability Discussion: Remote access services, such as those providing
remote access to network devices and information systems, which lack automated
control capabilities, increase risk and make remote user access management
difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized
user (or an information system) communicating through an external,

non-organization-controlled network. Remote access methods include, for example,
dial-up, broadband, and wireless.

Operating system functionality (e.g., RDP) must be capable of taking enforcement
action if the audit reveals unauthorized activity. Automated control of remote
access sessions allows organizations to ensure ongoing compliance with remote
access policies by enforcing connection rules of remote access applications on a
variety of information system components (e.g., servers, workstations, notebook
computers, smartphones, and tablets).

Responsibility: N/A
IAControls: N/A

Check Content:

Refer the TCP/IP PROFILE DD statement to determine the TCP/IP Ports. If the
PROFILE DD statement is not supplied, use the default search order to find the
PROFILE data set.

See the IP Configuration Guide for a description of the search order for
PROFILE.TCPIP.

If the all the Ports included in the configuration are restricted to the ports,
protocols, and/or services, as defined in the Ports, Protocols, and Services
Management (PPSM) Category Assurance List (CAL) and vulnerability assessments,
this is not a finding.

Fix Text:
Configure TCP/IP PROFILE port definitions to adhere to ports, protocols, and/or
services, as defined in the Ports, Protocols, and Services Management (PPSM)
Category Assurance List (CAL) and vulnerability assessments.

CCI: CCI-002314

Group ID (Vulid): V-223822
Group Title: TC000030
Rule ID: N/A
Severity: CAT II

Rule Version (STIG-ID): TC000030
Rule Title: The permission bits and user audit bits for HFS objects that are
part of the Base TCP/IP component must be configured properly.

Vulnerability Discussion: HFS directories and files of the Base TCP/IP component provide the configuration, operational, and executable properties of
IBMs TCP/IP system product. Failure to properly secure these objects may lead to
unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
permission
bits and user audit bits for HFS objects that are part of the Base TCP/IP component are
configured according to the settings in the following table:

DIRECTORY or FILE	PERMISSION BITS	USERAUDIT BITS
/etc/hosts	0744	faf
/etc/protocol	0744	faf
/etc/resolv.conf	0740	faf
/etc/services	0740	faf
/usr/lpp/tcpip/sbin	0755	faf
/usr/lpp/tcpip/bin	0755	faf

a) Using Vanguard Administrator UNIX File Manager option 14. Review all files
located in the table above.

b) If the HFS permission bits and user audit bits for each directory and file
match or
are more restrictive than the specified settings listed in this table, there is
NO
FINDING.

NOTE: Some of the files listed above are not used in every configuration. Absence of a file will not be 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

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

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or
SUPERUSER access, will review the UNIX permission bits and user audit bits on
the HFS directories and files for the Base TCP/IP component. Ensure they conform
to the specifications in the BASE TCP/IP HFS Object Security Settings below:

BASE TCP/IP HFS Object Security Settings

File	Permission Bits	User Audit Bits
/etc/hosts	0744	faf
/etc/protocol	0744	faf
/etc/resolv.conf	0744	faf
/etc/services	0740	faf
/usr/lpp/tcpip/sbin	0755	faf
/usr/lpp/tcpip/bin	0755	faf

Some of the files listed above (e.g., /etc/resolv.conf) are not used in every
configuration. While the absence of a file is generally not a security issue,
the existence of a file that has not been properly secured can often be an
issue. Therefore, all directories and files that do exist will have the
specified permission and audit bit settings.

The following represents a hierarchy for permission bits from least restrictive
to most restrictive:

```
7       rwx             (least restrictive)
6       rw-
3       -wx
```

```
2       -w-
5       r-x
4       r--
1       --x
0       ---             (most restrictive)
```

The possible audit bits settings are as follows:

```
f       log for failed access attempts
a       log for failed and successful access
-       no auditing
```

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 0744 /etc/hosts
chaudit w=sf,rx+f /etc/hosts
chmod 0744 /etc/protocol
chaudit w=sf,rx+f /etc/protocol
chmod 0744 /etc/resolv.conf
chaudit w=sf,rx+f /etc/resolv.conf
chmod 0740 /etc/services
chaudit w=sf,rx+f /etc/services
chmod 0755 /usr/lpp/tcpip/bin
chaudit w=sf,rx+f /usr/lpp/tcpip/bin
chmod 0755 /usr/lpp/tcpip/sbin
chaudit w=sf,rx+f /usr/lpp/tcpip/sbin
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223823
Group Title: TC000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TC000040
Rule Title: TCP/IP resources must be properly protected.

Vulnerability Discussion: The Communication Server access authorization is used to protect TCP/IP resources such as stack, network, port, and other SERVAUTH resources. These resources provide additional security checks for TCP/IP users. Failure to properly secure these TCP/IP resources could lead to unauthorized user access resulting in the compromise of some system services and possible compromise of data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
The IAO will ensure that the generic resources EZA, EZB and IST are defined to
the SERVAUTH
resource class and no access is specified.

The IAO will ensure that only authenticated users are permitted access to the
network
(NETACCESS), port (PORTACCESS), stack (STACKACCESS), CSSMTP, and FTP resources
in
the SERVAUTH class.

The IAO will ensure that the default access to EZA, EZB and IST -prefixed resources in the
SERVAUTH class is no access.

NOTE: This FINDING only pertains to domains running Z/OS Version 2 Release 10 or
above, including all releases of z/OS. If the domain being reviewed is not
running at the
required OS release, this FINDING will be marked NOT APPLICABLE.

a) Using Vanguard Administrator General Resource Profile report option 3;4. Mask
on class = SERVAUTH

b) Ensure the following items are in effect for Server Access Authorization
resources:

1. The following resources are defined to the SERVAUTH resource class with a
UACC(NONE):

EZA.**
EZA.FTP.**
EZA.NETACCESS.**
EZA.PORTACCESS.**
EZA.STACKACCESS.**

EZB.**
EZB.FTP.**
EZB.NETACCESS.**
EZB.PORTACCESS.**
EZB.STACKACCESS.**
If CSSmtp is on the system, the following resource must be defined for use by
the CSSMTP started task and authenticated users for email services:

EZB.CSSMTP.sysname.writername.JESnode

IST.**
IST.FTP.**
IST.NETACCESS.**
IST.PORTACCESS.**
IST.STACKACCESS.**

2. No access is granted to, EZA.**, EZB.** AND IST.** (EZA.**, EZB.**, IST.**
must be defined).
If the product CSSMTP is on the system, no acces is given to EZB.CSSMTP

3. Only authenticated users are permitted access to the network (NETACCESS),
port (PORTACCESS), stack (STACKACCESS), and FTP resources in the
SERVAUTH resource class and email services (
EZB.CSSMTP.sysname.writername.JESnode)
if CSSMTP is on the system Authenticated user access is indicated by ID(*)
access of READ in the access list (this should not be true for EZA.**,EZB.** AND
IST.** which
cannot have any entries in the access list).
4. Ensure that the profile WARNING flag is OFF.

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: The IAO must develop a plan of action to implement the required changes. Ensure the following items are in effect for TCP/IP resources.

(Note: The resource class, resources, and/or resource prefixes identified below
are examples of a possible installation. The actual resource class, resources,
and/or resource prefixes are determined when the product is actually installed
on a system through the product s installation guide and can be site specific.)

Ensure that the EZA, EZB and IST resources and/or generic equivalent are defined
to the SERVAUTH resource class with a UACC(NONE)

No access is given to the EZA, EZB, and IST resources of the SERVAUTH resource
class.

If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the
SERVAUTH resource class. EZB.CSSMTP.sysname.writername.JESnode will be specified
and made available to the CSSMTP started task and authenticated users that
require access to use CSSMTP for e-mail services.

Only authenticated users that require access are permitted access to the second
level of the resources in the SERVAUTH resource class. Examples are the network
(NETACCESS), port (PORTACCESS), stack (STACKACCESS), and FTP resources in the
SERVAUTH resource class.

The EZB.STACKACCESS. resource access authorizations restrict access to those
started tasks with valid requirements and users with valid FTP access requirements.

The EZB.FTP.*.*.ACCESS.HFS) resource access authorizations restrict access to
FTP users with specific written documentation showing a valid requirement exists
to access OMVS files and Directories.

The following commands are provided as a sample for implementing resource controls:

```
RDEF SERVAUTH EZB.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.sysname.writername.JESnode UACC(NONE)
OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.FTP.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.NETACCESS.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.PORTACCESS.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.STACKACCESS.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))

PE EZB.CSSMTP.sysname.writername.JESnode CL(SERVAUTH) ID(authusers)
ACC(READ)
PE EZB.FTP.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.sysname.ftpstc.ACCESS.HFS CL(SERVAUTH) ID(ftpprofile)
ACC(READ)
PE EZB.NETACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.PORTACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.sysname.TCPIP CL(SERVAUTH) ID(ftpprofile) ACC(READ)
```

The following notes apply to these controls:

- EZB.STACKACCESS.sysname.TCPIP access READ should be limited to only those started tasks that require access to the TCPIP Stack as well as any users approved for FTP Access (inbound and/or outbound). FTP users should not have access to the EZB.FTP.sysname.ftpstc.ACCESS.HFS resource unless specific written justification documenting valid requirement for those FTP users to access USS files and directories via FTP.

- To be effective in restricting access, the network (EZB.NETACCESS) resource control requires configuration of the NETACCESS statement in the PROFILE.TCPIP file.

- To be effective in restricting access, the port (EZB.PORTACCESS) resource control requires configuration of a PORT or PORTRANGE statement in the PROFILE.TCPIP file. These port definitions within PROFILE.TCPIP shall be defined to include SAF keyword and a valid name.

A list of possible SERVAUTH resources defined to the first two nodes is shown here: (Note that additional resources may be developed with each new release of TCPIP.)

EZA.DCAS.
EZB.BINDDVIPARANGE.
EZB.CIMPROV.
EZB.FRCAACCESS.
EZB.FTP.
EZB.INITSTACK.
EZB.IOCTL.
EZB.IPSECCMD.
EZB.MODDVIPA.
EZB.NETACCESS.
EZB.NETMGMT.
EZB.NETSTAT.
EZB.NSS.
EZB.NSSCERT.
EZB.OSM.
EZB.PAGENT.
EZB.PORTACCESS.
EZB.RPCBIND.
EZB.SOCKOPT.
EZB.SNMPAGENT.
EZB.STACKACCESS.
EZB.TN3270.
IST.NETMGMT.

CCI: CCI-000213

Group ID (Vulid): V-223824
Group Title: TC000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TC000050
Rule Title: The RACF SERVAUTH resource class must be active for TCP/IP resources.

Vulnerability Discussion: IBM Provides the SERVAUTH Class for use in protecting
a variety of TCP/IP features/functions/products both IBM and third-party. Failure to activate this class will result in unprotected resources. This exposure may threaten the integrity of the operating system environment, and
compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
NOTE: The procedures in this checklist item presume the domain being reviewed is
running all releases of z/OS, and use the ACP as the certificate store.

The IAO will ensure that for production environments, expired certificates are
not used.

If the domain being reviewed is not a production system and is only used for
test and development, Expired Certificates review can be skipped.

RACDCERT ID(tcpip userid) LIST

a) 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.

b) 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.

CCI: CCI-000068

Group ID (Vulid): V-223826
Group Title: TC000070
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TC000070
Rule Title: MVS data sets for the Base TCP/IP component are not properly protected,

Vulnerability Discussion: MVS data sets of the Base TCP/IP component provide
the configuration, operational, and executable properties of IBMs TCP/IP system
product. Failure to properly secure these data sets may lead to unauthorized
access resulting in the compromise of the integrity and availability of the
operating system environment, ACP, and customer data.

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

Check Content:
The IAO will ensure that update, create, and scratch access to product data sets
are
restricted to systems programming personnel.

The IAO will ensure that update, create, and scratch access to the data set(s)
containing
the TCPIP.DATA and PROFILE.TCPIP configuration files are restricted to systems
programming personnel and are logged.

The IAO will ensure that update, create, and scratch access to the data set(s)
containing
the configuration files shared by TCP/IP applications are restricted to systems
programming personnel.

The IAO will ensure that write and allocate access to the data set(s) specified
in the

INCLUDE statements are restricted to systems programming personnel and are
logged.

a) Display the active started tasks executing on the domain using SDSF, or
equivalent JES display product, and locate the TCPIP started task. Locate and
document the configuration file identified by the PROFILE DD statement. Locate
and document the Data File identified by the SYSTCPD DD statement.
 NOTE: Record the covering dataset profile for use in later steps.

b) Ensure the following controls are in effect for the Base TCP/IP component:
1. Using Vanguard Administrator On-line Access and Authorization option
4. Supply the datasets documented above and ensure UPDATE and
ALTER access to product data sets is restricted to systems programming
personnel (i.e., SMP/E distribution data sets with the prefix
SYS1.TCPIP.AEZA and target data sets with the prefix
SYS1.TCPIP.SEZA).

2. Using Vanguard Administrator On-line Access and Authorization option
4. Supply the dataset names documented above. Review the access and
ensure UPDATE and ALTER access to the data set(s) containing the Data
and Profile configuration file is restricted to systems programming
personnel.

NOTE: If any INCLUDE statements are specified in the Profile configuration file,
the named MVS data sets have the same access authorization requirements.

3. Using Vanguard Administrator Audit Flags Report option 3;3;2. Supply
the datasets documented above. All UPDATE and ALTER access to the
data set(s) containing the Data and Profile configuration files is
logged.

NOTE: If any INCLUDE statements are specified in the Profile configuration file,
the named MVS data sets have the same logging requirements.

4. Using Vanguard Administrator On-line Access and Authorization option
4. Supply the dataset name for the configuration file documented above.
Review the access and ensure UPDATE and ALTER access to the data
set(s) containing the configuration files shared by TCP/IP applications is
restricted to systems programming personnel.

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

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

Fix Text: Review with the IAO the data set access authorizations defined to the

ACP for the Base TCP/IP component. Ensure these data sets are protected in
accordance with the following rules:

WRITE and ALLOCATE access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix SYS1.TCPIP.AEZA and target data sets with the prefix SYS1.TCPIP. SEZA).

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile
configuration files is restricted to systems programming personnel.

NOTE: If any INCLUDE statements are specified in the Profile configuration
file, the named MVS data sets have the same access authorization requirements.

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile
configuration files is logged.

NOTE: If any INCLUDE statements are specified in the Profile configuration
file, the named MVS data sets have the same logging requirements.

WRITE and ALLOCATE access to the data set(s) containing the configuration files
shared by TCP/IP applications is restricted to systems programming personnel.

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-223829
Group Title: TC000100
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TC000100
Rule Title: TCPIP.DATA configuration statements for the TCP/IP stack will be
properly specified.

Vulnerability Discussion: During the initialization of TCP/IP servers and clients, the TCPIP.DATA configuration file provides information that is essential for proper operations of TCP/IP applications. Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the TCPIPJOBNAME, HOSTNAME, DOMAINORIGIN, DATASETPREFIX, and NSINTERADDR statements are coded in the TCPIP.DATA file.

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP.DATA configuration file.

b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Data configuration file:

1. TCPIPJOBNAME
2. HOSTNAME
3. DOMAINORIGIN/DOMAIN (The DOMAIN statement is functionally equivalent to the DOMAINORIGIN Statement)
4. DATASETPREFIX

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

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

Fix Text: The system programmer will review the configuration statements in the TCPIP.DATA file and ensure they conform to the specifications below:

TCPIPJOBNAME - Specifies the job name of the TCP/IP address space. This name is also used as part of the name of some network security resources.

HOSTNAME - Specifies the TCP/IP host portion of the DNS name of the system.

DOMAINORIGIN/DOMAIN - Specifies the default domain name used for DNS searches.

DATASETPREFIX - Specifies the high-level qualifier to be used to dynamically
allocate other configuration data sets.

The TCPIP.DATA file acts as the anchor configuration data set for the TCP/IP
stack and all TCP/IP servers and clients running in z/OS. During the initialization of TCP/IP servers and clients, the TCPIP.DATA file provides basic
information that is essential for proper operation.

The above TCPIP.DATA configuration parameters provide crucial information to
TCP/IP applications.

CCI: CCI-000366

Group ID (Vulid): V-252553
Group Title: TC000110
Rule ID: SV-00000r0_rule
Severity: CAT II
Rule Version (STIG-ID): TC000110
Rule Title: IBM z/OS TCP/IP AT-TLS policy must be properly configured in Policy
Agent.

Vulnerability Discussion: If events associated with nonlocal administrative
access or diagnostic sessions are not logged, a major tool for assessing and
investigating attacks would not be available.

This requirement addresses auditing-related issues associated with maintenance
tools used specifically for diagnostic and repair actions on organizational
information systems.

Nonlocal maintenance and diagnostic activities are conducted by individuals
communicating through an external network (e.g., the internet) or an internal
network. Local maintenance and diagnostic activities are carried out by individuals physically present at the information system or information system
component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or
tools. This requirement does not cover hardware/software components that may
support information system maintenance, yet are a part of the system; for example, the software implementing "ping," "ls," "ipconfig," or the hardware and
software implementing the monitoring port of an Ethernet switch.

Responsibility: Systems Programmer
IAControls: n/a

Check Content:

Use the z/OS UNIX pasearch -t command to query information from the z/OS UNIX
Policy Agent.

The command is issued from the UNIX System Services shell.

Examine the results for AT-TLS initiation and control statements.

If there are no AT-TLS initiation and controls statements this is a finding.

Verify the statements specify a FIPS 140-2 compliant value. If none of the
following values are present, this is a finding

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

Fix Text:
Develop a plan of action to implement the required changes. Ensure the following
items are in effect for TCP/IP resources.

Develop AT-TLS policy. Install in the policy agent.

Ensure that the statements specify a FIPS 140-2 compliant value of the following
values.

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

CCI: CCI-000067

Group ID (Vulid): V-223831
Group Title: TN000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TN000020
Rule Title: SSL encryption options for the TN3270 Telnet Server will be specified properly for each statement that defines a SECUREPORT or within the
TELNETGLOBALS.

Vulnerability Discussion: During the SSL connection process a mutually acceptable encryption algorithm is selected by the server and client. This
algorithm is used to encrypt the data that subsequently flows between the two.
However, the level or strength of encryption can vary greatly. Certain configuration options can allow no encryption to be used and others can allow a
relatively weak 40-bit algorithm to be used. Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECMT-2, ECTM-1

Check Content:
The systems programmer responsible for supporting ICS will ensure that a TELNETPARMS ENCRYPTION statement is coded for each statement block that defines a SECUREPORT.

The systems programmer responsible for supporting ICS will ensure that to prevent the
use of null or 40-bit encryption, each TELNETPARMS ENCRYPTION statement does
not specify any of the following operands: SSL_NULL_Null, SSL_NULL_MD5, SSL_NULL_SHA, SSL_RC4_MD5_EX, or SSL_RC2_MD5_EX.

a) Using SDSF or equivalent to locate the Profile configuration file specified
on the
PROFILE DD statement in the TCPIP started task JCL or the TN3270 started task if configure separately in z/OS 1.8 and above.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

b) From the ISPF Primary Option Menu use option 3.4 and review the profile
configuration file and ensure the following items are in effect for the
configuration statements specified in the Profile configuration file:

1. Within each TELNETPARMS block that specifies a SECUREPORT
statement, an ENCRYPTION statement is also coded.
2. To prevent the use of non FIPS 140-2 encryption, each TELNETPARMS
ENCRYPTION statement will specify any or all of the following
operands:
a. SSL_3DES_SHA
b. SSL_AES_256_SHA
c. SSL_AES_128_SHA

c) If both (B)1. and (B)2. of the above are true, there is NO FINDING.

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

Fix Text: The IAO will ensure the system programmer will review the SECUREPORT
and TELNETPARMS ENCRYPTION statements and/or the TELNETGLOBALS statement in the
PROFILE.TCPIP file. Ensuring that they conform to the requirements specified
below.

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

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

To prevent the use of non FIPS 140-2 encryption, the TELNETGLOBALS block and/or
each TELNETPARMS block that specifies an ENCRYPTION statement will specify one
or more of the following cipher specifications:

Cipher Specifications
SSL_3DES_SHA
SSL_AES_256_SHA
SSL_AES_128_SHA

Note: Always check for the minimum allowed in FIPS 140-2.

CCI: CCI-000068

CCI: CCI-002450

Group ID (Vulid): V-223833
Group Title: TN000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TN000040
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 adver

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:

The systems programmer responsible for supporting ICS will ensure that all USS
tables
referenced in BEGINVTAM USSTCP statements includes MSG10 text that specifies a
warning logon banner.

a) Display the active started tasks executing on the domain using SDSF, or
equivalent JES display product, and locate the TCPIP started task. Locate the
TCPIP configuration file identified by the PROFILE DD statement. From the
ISPF Primary Option Menu use option 3.4 and review the TCPIP Date
configuration file.

b) Ensure that all USS tables referenced in BEGINVTAM USSTCP statements
include MSG10 text that specifies a logon banner. The below banner is mandatory
and deviations are not permitted except as authorized in writing by the DoD

Chief
Information Officer. The thrust of this new policy is to make it clear that
there is
no expectation of privacy when using DoD information systems and all use of
DoD information systems is subject to searching, auditing, inspecting, seizing,
and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided
for USG-authorized use only. By using this IS (which includes any device attached to this
IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to
routine
monitoring, interception, and search, and may be disclosed or used for any USG
authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to
protect
USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI
investigative searching or monitoring of the content of privileged communications, or
work product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product
are private and confidential. See User Agreement for details.

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

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

Fix Text:
Review all USS tables referenced in BEGINVTAM USSTCP statements in the PROFILE.TCPIP file. Ensure the MSG10 text specifies a logon banner in accordance
with DISA requirements. See MGG10 below:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement (LE),
and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services
by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement
for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet
Server, the banner can be implemented through the USS table that is specified on
a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e.,

MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

CCI: CCI

CCI: CCI-001384CCI

CCI: CCI-001385CCI

CCI: CCI-001386CCI

CCI: CCI-001387CCI

CCI: CCI-001388

Group ID (Vulid): V-223834
Group Title: TN000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TN000050
Rule Title: VTAM session setup controls for the TN3270 Telnet Server are not
properly specified.

Vulnerability Discussion: After a connection from a Telnet client to the TN3270
Telnet Server has been established, the process of session setup with a VTAM
application occurs. A number of BEGINVTAM statements must be coded in a specific
configuration to ensure adequate control to VTAM applications is maintained.
Failure to code the appropriate statements could result in unauthorized access
to the host and application resources. This exposure may impact data integrity
or the availability of some system services.

Documentable: YES
Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that within
each

BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. The named table allows access only to
session
manager applications and NC-PASS applications. This USSTCP statement does not
specify any type of client identifier, such as host name or IP address, so that
the statement
applies to all connections not otherwise controlled.

The systems programmer responsible for supporting ICS will ensure that within
each
BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications are coded only if
the
statements include a client identifier operand that references only secure
terminals.

The systems programmer responsible for supporting ICS will ensure that any
BEGINVTAM DEFAUTLAPPL statement that does not specify a client identifier, or
specifies any type of client identifier that would apply to unsecured terminals,
specifies a
session manager application or an NC-PASS application as the application name.

The systems programmer responsible for supporting ICS will ensure that for
systems at
Z/OS Release 2.10 and above, any BEGINVTAM LUMAP statement, if used with the
DEFAPPL operand and applied to unsecured terminals, specifies only a session
manager
application or an NC-PASS application.

a) Display the active started tasks executing on the domain using SDSF, or
equivalent JES display product, and locate the TCPIP started task. Locate the
TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP Data configuration file.

b) Ensure the following items are in effect for the configuration statements
specified

in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

1. Within each BEGINVTAM statement block, one BEGINVTAM USSTCP
statement is coded that specifies only the table name operand. No client
identifier, such as host name or IP address, is specified so the statement
applies to all connections not otherwise controlled.

2. The USS table specified on each back stop USSTCP statement mentioned in
Item (1) above is coded to allow access only to session manager applications
and NC-PASS applications. This check requires Manual Review.

3. Within each BEGINVTAM statement block, additional BEGINVTAM
USSTCP statements that specify a USS table that allows access to other
applications may be coded only if the statements include a client identifier
operand that references only secure terminals.

4. Any BEGINVTAM DEFAULTAPPL statement that does not specify a client
identifier, or specifies any type of client identifier that would apply to
unsecured terminals, specifies a session manager application or an NC-PASS
application as the application name. This check requires Manual Review. IBM
Communications Server Data Analysis

5. Any BEGINVTAM LUMAP statement, if used with the DEFAPPL operand
and applied to unsecured terminals, specifies only a session manager
application or an NC-PASS application. This check requires Manual Review.

NOTE: The BEGINVTAM LINEMODEAPPL requirements will not be
reviewed at this time. Further testing must be performed to determine how the
CL/Supersession and NC-PASS applications work with line mode.

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

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

Fix Text: Review the BEGINVTAM configuration statements in the PROFILE.TCPIP
file. Ensure they conform to the specifications
below.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration
file, the data set specified on this statement must be checked for the following
items as well.

Within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded
that specifies only the table name operand. No client identifier, such as host
name or IP address, is specified so the statement applies to all connections not
otherwise controlled.

The USS table specified on each back stop USSTCP statement mentioned above is
coded to allow access only to session manager applications and NC PASS applications

Within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements
that specify a USS table that allows access to other applications may be coded
only if the statements include a client identifier operand that references only
secure terminals.

Any BEGINVTAM DEFAULTAPPL statement that does not specify a client identifier,
or specifies any type of client identifier that would apply to unsecured
terminals, specifies a session manager application or an NC PASS application as
the application name

For z/OS systems, any BEGINVTAM LUMAP statement, if used with the DEFAPPL
operand and applied to unsecured terminals, specifies only a session manager
application or an NC PASS application.

Further explanation:

After a connection from a Telnet client to the TN3270 Telnet Server has been
established, the process of session setup with a VTAM application occurs. A
number of BEGINVTAM statements will be coded in a specific configuration to
ensure that adequate control over access to VTAM applications is maintained.

Connections originate from secure terminals or unsecured terminals. The TN3270

Telnet Server should be configured to address these two types of connections.
Terminals should meet two conditions to be considered secure. One condition
involves the hardware and configuration. Secure terminals include devices that
are directly attached to the host, such as 3270-type terminals coax connected to
a 3174 Control Unit. They also include PCs running 3270 terminal emulation
clients attached to a private LAN (i.e., a LAN without access to an external
network such as the NIPRNet). The other condition involves the location of the
terminals. Secure terminals are located in areas with physical access limited to
authorized personnel. Examples of terminals that are not secure are those
attached via the NIPRNet or via dial-in servers. The intent of this distinction
is to allow additional connection options (e.g., bypassing session manager
control) to authorized personnel working in controlled access areas. These
connection options may be necessary for operational control or for system
recovery procedures.

The BEGINVTAM USSTCP statement can be used to specify a customized Unformatted
System Services (USS) table for client connections. The USS table can provide a
level of access control by restricting the commands that allow connections to
VTAM applications. The USS table specified by the USSTCP statement can be the
same as the one used by the SNA component of IBM Communications Server.

The BEGINVTAM DEFAULTAPPL statement can be used to specify the VTAM application
to which a client is automatically connected when a session is established using
a protocol other than linemode protocol.

The BEGINVTAM LUMAP statement can specify a default VTAM application using the
DEFAPPL operand. This processing is similar to the DEFAULTAPPL and LINEMODEAPPL
processing, except that a client identifier should be coded. When a client
matches the LUMAP specification, the DEFAPPL specification overrides the
DEFAULTAPPL or LINEMODEAPPL specifications.

CCI: CCI-000366

Group ID (Vulid): V-223835
Group Title: TN000060
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TN000060
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 syst

Responsibility: Systems Programmer
IAControls: N/A

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-223836
Group Title: TS000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): TS000010
Rule Title: TSOAUTH resources must be restricted to authorized users.

Vulnerability Discussion: The TSOAUTH resource class controls sensitive privileges, such as OPER, ACCOUNT, CONSOLE, and PARMLIB. Several of these privileges offer the ability, or provide a facility, to modify sensitive operating system resources. Failure to properly control and restrict access to
these privileges may result in the compromise of the operating system environment, ACP, and customer data.

Potential Impacts:
fix typo error

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

Check Content:
a) From Administrator main menu, go to 3;4;

b) In the Batch/On-line field key in B. In the Class field key in TSOAUTH. On
the
command line key in 4 (for the Access Lists report). Press ENTER. Accept the
processing options by pressing <ENTER>. Submit the report.

c) Review the GENERAL RESOURCE ACCESS LISTS report ensuring the following items are in effect:
1. The ACCT authorization is restricted to security personnel.

2. The CONSOLE authorization is restricted to authorized and READ access may be
given to all user when SDSF is installed at the IAOs discretion.
systems personnel (e.g., systems programming personnel, operations staff, etc.).
3. The MOUNT authorization is not granted to on-line TSO users
4. The OPER authorization is restricted to authorized systems personnel (e.g.,
systems programming personnel, operations staff, etc.).
5. The PARMLIB authorization is restricted to only systems programming personnel and READ access may be given to audit users.

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

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

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 in install 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-223837
Group Title: TS000020
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): TS000020
Rule Title: LOGONIDs must not be defined to SYS1.UADS for non-emergency use.

Vulnerability Discussion: SYS1.UADS is a dataset where LOGONIDs will be maintained with applicable password information when the ACP is not functional.
If an unauthorized user has access to SYS1.UADS, they could enter their LOGONID
and password into the SYS1.UADS dataset and could give themselves all special
attributes on the system. This could enable the user to bypass all security and
alter data. They could modify the audit trail information so no trace of their
activity could be found.

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

Check Content:
a) From Analyzer main menu, go to 4;U.
Note: Analyzer 8.1 with PTF VS48081 is required for this option to be available.

b) Set Exceptions only field to NO. Press ENTER.

c) Submit the report.

d) Review the generated report.

e) If SYS1.UADS userids are limited and reserved for emergency purposes only,
there is NO FINDING.

f) If any SYS1.UADS userids are assigned for other than emergency purposes, this
is a FINDING.

Fix Text: The system programmer and IAO will examine the SYS1.UADS entries to
ensure LOGONIDs defined include only those users required to support specific
functions related to system recovery. Evaluate the impact of accomplishing the
change.

CCI: CCI-000764

Group ID (Vulid): V-223838
Group Title: US000010
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): US000010
Rule Title: z/OS UNIX SUPERUSER resource must be protected in accordance with
guidelines.

Vulnerability Discussion: z/OS UNIX ACP-defined resources consist of sensitive
capabilities including SUPERUSER, daemon, and numerous file manipulation
privileges. Missing or inaccurate protection of these resources could allow a
user to access sensitive data, modify or delete data and operating system
controls, or issue commands that could negatively impact system
availability.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
The IAO will ensure that the CHOWN.UNRESTRICTED resource is not defined, unless
a
letter justifying access is filed with the IAO. The IAO will ensure that all
SUPERUSER
resources for the UNIXPRIV resource class are restricted to appropriate system
tasks
and/or system programming personnel, unless a letter justifying access is filed
with the
IAO. And the IAO will ensure that all SUPERUSER resources for the UNIXPRIV
resource class have default access of none.

a) Using Vanguard Administrator General Resource Report s option 3; 4 to review
profiles listed below. Use Class masking UNIXPRIV and browse the profile listed
below.

b) Review the following items for the UNIXPRIV resource class:
1. The RACF rules for the SUPERUSER resource specify a default access of NONE.
2. There are no RACF rules that allow access to the SUPERUSER resource.
3. There is no RACF rule for CHOWN.UNRESTRICTED defined.

4. The RACF rules for each of the SUPERUSER resources listed in listed in the
UNIXPRIV CLASS RESOURCES Table in the z/OS STIG Addendum, specify a default
access of
NONE.
5. The RACF 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: Ensure that all SUPERUSER resources for the UNIXPRIV resource class
are restricted to appropriate system tasks and/or system programming
personnel.

1) The RACF rules for the SUPERUSER resource specify a default access of
NONE.

2) There are no RACF rules that allow access to the SUPERUSER resource.

3) There is no RACF rule for CHOWN.UNRESTRICTED defined.

4) The RACF rules for each of the SUPERUSER resources listed in the
UNIXPRIV CLASS RESOURCES Table in the z/OS STIG Addendum, specify a default
access of NONE.

5) The RACF 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:

```
RDEF UNIXPRIV SUPERUSER.** UACC(NONE) OWNER(ADMIN) DATA('REFERENCE
ZUSS0023')
AUDIT(ALL(READ))
/* do not permit any users/groups to this resource */

SR CLASS(UNIXPRIV) MASK(CHOWN.UNRESTRICTED)
/* delete if found */

PE SUPERUSER.FILESYS.** CL(UNIXPRIV) ID(<SYSPAUDT>)
/* where SUPERUSER.FILESYS.** represents one of the resources listed in
the
UNIXPRIV CLASS RESOURCES table in the Addendum */
```

CCI: CCI-000213

CCI: CCI-001764

Group ID (Vulid): V-223839
Group Title: US000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000020
Rule Title: BPX resource(s)s is(are) not protected in accordance with security
requirements.

Vulnerability Discussion: z/OS UNIX ACP-defined resources consist of sensitive
capabilities including SUPERUSER, daemon, and numerous file manipulation privileges. Missing or inaccurate protection of these resources could allow a
user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:
The Systems Programmer and IAO will ensure that BPX. Resources are properly
protected and access is restricted to appropriate system tasks or systems programming
personnel, unless a letter justifying additional access is filed with the IAO.
The Systems
Programmer and IAO will ensure that BPX. DAEMON resources are properly protected
and access is restricted to appropriate system tasks or systems programming
personnel,
unless a letter justifying additional access is filed with the IAO

a) Use Vanguard Administrator General Resource Report option 3;4 to review the
FACILITY Class. Use Class Facility and Profile BPX.*.** for the masking.

b) Review the following items for the FACILITY resource class, TYPE(FAC):

1. The RACF rules for the BPX.** resource specify a default access of NONE.

2. There are no RACF user access to the BPX.** resource.

3. There is no RACF rule for BPX.SAFFASTPATH defined.

4. The RACF rules for each of the BPX resources listed in the General Facility
Class BPX Resources Table in the z/OS STIG Addendum specify a default access of
NONE.

5. The RACF rules for each of the BPX resources listed in the General Facility
Class BPX Resources Table in the z/OS STIG Addendum GENERAL FACILITY CLASS BPX
Resources, 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: There are a number of resources available under z/OS UNIX that must be
secured in order to preserve system integrity while allowing effective
application and user access. All of these resources might not be used in every
configuration, but several of them have critical impacts.

The default access for each of these resources must be no access. A generic
resource (e.g., BPX.**) must also be set to a default access of none to cover
future additions. Because they convey especially powerful privileges, the
settings for BPX.DAEMON, BPX.SAFFASTPATH, BPX.SERVER, and BPX.SUPERUSER require
special attention.

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).

As noted above, the BPX.SAFFASTPATH definition can cause successful security
checks not to be audited. Because auditing of all accesses is required for some
system files, BPX.SAFFASTPATH must not be used.

Access to BPX.SERVER must be restricted to system software processes that act as
servers under z/OS UNIX (e.g., web servers).

Access to BPX.SUPERUSER must be restricted to Security Administrators and individual systems programming personnel. It is not appropriate for all systems
programming personnel, only for those with responsibilities for components or
products that use z/OS UNIX and that require superuser capability for maintenance.

1) The RACF rules for the BPX.** resource specify a default access of
NONE.
2) There are no RACF user access to the BPX.** resource.
3) There is no RACF rule for BPX.SAFFASTPATH defined.
4) The RACF rules for each of the BPX resources listed in "General Facility Class BPX Resources" table in the zOS STIG Addendum specify a UACC
value of NONE.
5) The RACF rules for each of the BPX resources listed in the "General
Facility Class BPX Resources" table in the zOS STIG Addendum restrict access to
appropriate system tasks or systems programming personnel as specified.

The following list of sample commands are provided to implement this requirement.

```
 rdef facility bpx.** uacc(none) owner(admin) audit(all(read)) -
data('see
zuss0021')
 rdef facility bpx.daemon uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
 pe bpx.daemon cl(facility id(<authorized_users>)
 rdef facility bpx.debug uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
 pe bpx.debug cl(facility id(<authorized_users>)
 rdef facility bpx.fileattr.apf uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
 pe bpx.fileattr.apf cl(facility id(<authorized_users>)
 rdef facility bpx.fileattr.progctl uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
 pe bpx.fileattr.progctl cl(facility id(<authorized_users>)
 rdef facility bpx.jobname uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
 pe bpx.jobname cl(facility id(<authorized_users>)
rdef facility bpx.server uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
pe bpx.server cl(facility id(<authorized_users>)
rdef facility bpx.smf uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
pe bpx.smf cl(facility id(<authorized_users>)
rdef facility bpx.stor.swap uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
pe bpx.stor.swap cl(facility id(<authorized_users>)
```

```
rdef facility bpx.superuser uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
pe bpx.superuser cl(facility id(<authorized_users>)
rdef facility bpx.wlmserver uacc(none) owner(admin) -
 audit(all(read)) data('see zuss0021')
pe bpx.wlmserver cl(facility id(<authorized_users>)
```

CCI: CCI-000213

CCI: CCI-001764

Group ID (Vulid): V-223840
Group Title: US000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000030
Rule Title: z/OS UNIX MVS HFS directory(s) with "other" write permission bit set
are not properly defined.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data
sets that contain operating system components, MVS data sets that contain HFS
file systems with operating system components, and MVS data sets that contain
HFS file systems with application system and user data. All of these MVS data
sets require definitions in the ACP to enforce desired access controls. In
addition, the UNIX permission bits must be properly set on the HFS directories
and files to enforce desired access controls.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECCD-1, ECCD-2

Check Content:
The Systems Programmer will ensure that the HFS directory(ies) with the "other"
write
permission bit set is (are) not properly defined.

a) If there are no directories that have the other write permission bit set on
without
the sticky bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a t
or T

in the execute portion of the other permissions. For example, a display of the
permissions
of a directory with the sticky bit on could be drwxrwxrwt .

b) If all directories that have the other write permission bit set on do not
contain any
files with the setuid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an
s or
S in the execute portion of the owner permissions. For example, a display of
the
permissions of a file with the setuid bit on could be -rwsrwxrwx .

c) If all directories that have the other write permission bit set on do not
contain any
files with the setgid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an
s or S
in the execute portion of the group permissions. For example, a display of the
permissions
of a file with the setgid bit on could be -rwxrwsrwx .

d) If (a), (b), or (c) above is untrue, this is a FINDING.

Fix Text: The systems programmer will verify the following:

b) There are no directories that have the other write permission bit set
on without the sticky bit set on.

NOTE: In the symbolic permission bit display, the sticky bit is indicated
as a t or T in the execute portion of the other permissions. For example, a
display of the permissions of a directory with the sticky bit on could be
drwxrwxrwt .

c) All directories that have the other write permission bit set on do not
contain any files with the setuid bit set on.

NOTE: In the symbolic permission bit display, the setuid bit is indicated
as an s or S in the execute portion of the owner permissions. For example, a
display of the permissions of a file with the setuid bit on could be -rwsrwxrwx
.

d) All directories that have the other write permission bit set on do not
contain any files with the setgid bit set on.

NOTE: In the symbolic permission bit display, the setgid bit is indicated
as an s or S in the execute portion of the group permissions. For example, a
display of the permissions of a file with the setgid bit on could be -rwxrwsrwx
.

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-223842
Group Title: US000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000050
Rule Title: z/OS UNIX security parameters in etc/profile are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values
for z/OS UNIX security controls. The parameters impact HFS data access and
operating system services. Undesirable values can allow users to gain
inappropriate privileges that could impact data integrity or the availability of
some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The Systems Programmer will ensure 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.

a) Using Vanguard Administrator UNIX file manager option 14 open /etc directory
and brows the profile file

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-223843
Group Title: US000060
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000060
Rule Title: z/OS UNIX security parameters in /etc/rc not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The Systems Programmer will ensure that any chmod or chaudit command specified in the /etc/rc file does not result in less restrictive security than what is specified in System Directory Security Settings found in the U_zOS_STIG_Addendum. . The Systems Programmer will ensure that the_BPX_JOBNAME variable is set to match the daemon s name (e.g., inetd, syslogd)

a) Using Vanguard Administrator UNIX file manager option 14. Use the CD command to change to the /etc directory and browse the rc file.
b) If all of the chmod commands in /etc/rc do not result in less restrictive access than what is specified in the table entitled System Directory Security Settings and the table entitled System File Security Settings in table 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 table entitled System Directory Security Settings and the table
entitled System File Security Settings in Section 2.5.2.5, Z/OS UNIX HFS Directories and Files, of the 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.
Table 8 - System Directory Security Settings
Note: Any Directory that uses AUTOMOUNT, does not require the specified settings.

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 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-223844
Group Title: US000070
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): US000070
Rule Title: z/OS UNIX resources must be protected in accordance with security
requirements.

Vulnerability Discussion: z/OS UNIX ACP-defined resources consist of sensitive
capabilities including SUPERUSER, daemon, and numerous file manipulation
privileges. Missing or inaccurate protection of these resources could allow a
user to access sensitive data, modify or delete data and operating system
controls, or issue commands that could negatively impact system availability.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
he 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, unless a letter justifying additional access is filed
with the IAO.

a) Using Vanguard Administrator General Resource Report option 3;4 to review the
FACILITY Class. Use Class Facility and Profile BPX.SRV.** for the masking.

b) If the RACF rules for all BPX.SRV.user SURROGAT resources specify a default
access of NONE, there is NO FINDING.

c) If the RACF 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, there is NO FINDING.

d) If (b) or (c) above is untrue, this is a FINDING.

Fix Text: 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.

The default access for each BPX.SRV.userid resource must be no access. Access
can be permitted only to system software processes that act as servers under
z/OS UNIX (e.g., web servers).

1) RACF rules for all BPX.SRV.user SURROGAT resources must specify a
default access of NONE.

A sample is provided here:

RDEF SURROGAT BPX.SRV.user UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))

2) RACF rules for all BPX.SRV.user SURROGAT resources must restrict access
to system software processes (e.g., web servers) that act as servers under z/OS

UNIX.

```
RDEF SURROGAT BPX.SRV.user UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
PE BPX.SRV.user CL(SURROGAT) ID(<server>)
```

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223845
Group Title: US000080
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000080
Rule Title: z/OS UNIX MVS data sets or HFS objects are not properly protected.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

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

Check Content:
(ZUSS0031: CAT II) The Systems Programmer and IAO will ensure that data set rules for the data sets referenced in the ROOT and MOUNT statements in BPXPRMxx member in. PARMLIB are properly restricted and access is restricted to appropriate system tasks or systems programming personnel, unless a letter justifying additional access is filed with the IAO.

a) Use Vanguard Analyzer UNIX System Services Filesystems option 3;N to review
current UNIX System Mount points Use the R command to review the dataset rules for each profile listed below.

b) If the RACF 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 RACF 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-223846
Group Title: US000090

Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000090
Rule Title: z/OS UNIX MVS data sets WITH z/OS UNIX COMPONENTS are not properly protected

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

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

Check Content:
The Systems Programmer and IAO will ensure that data set rules for the data sets referenced in the table A-19 are properly restricted and UPDATE and/or ALLOCATE/ALTER access is restricted to systems programming personnel, unless a letter justifying additional access is filed with the IAO.

a) Use Vanguard Administrator Data Set Reports option 3;3 to review dataset profiles listed in the table above.

b) If the RACF data set rules for each of the data sets listed in Section 2.5.2.4.1 MVS Data Sets with Z/OS UNIX Components, Table A-19, of the Z/OS STIG restrict UPDATE and ALTER 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-223847
Group Title: US000100
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000100
Rule Title: z/OS UNIX HFS permission bits and audit bits for each directory will
be properly protected or specified.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data
sets that contain operating system components, MVS data sets that contain HFS
file systems with operating system components, and MVS data sets that contain
HFS file systems with application system and user data. All of these MVS data
sets require definitions in the ACP to enforce desired access controls. In
addition, the UNIX permission bits must be properly set on the HFS directories
and files to enforce desired access controls.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:
he Systems Programmer will ensure that the HFS permission bits for each directory
match or are more restrictive than the specified settings listed in the table
A-21 entitled
System Directory Security Settings in Section 2.5.2.5.1. found in the
U_zOS_STIG_Addendum

a) Use Vanguard UNIX file manager option 14 and review the files listed listed
in the SYSTEM DIRECTORY SECURITY SETTINGS Table in the z/OS STIG Addendum,

If the HFS permission bits for each directory match or are more restrictive than
the
specified settings listed in Section 2.5.2.5.1, Z/OS System HFS Directories,
Table A21, of
the Z/OS STIG, there is NO 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)

b) If the HFS user audit bits for each directory match or include the specified
settings
listed in Section 2.5.2.5.1, Z/OS System HFS Directories, Table A-21, of the
Z/OS
STIG, 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

c) If (b) or (c) above is untrue, this is a FINDING.

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or
SUPERUSER access, will review the UNIX permission bits and user audit bits on
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-223848
Group Title: US000110
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000110
Rule Title: z/OS UNIX SYSTEM FILE SECURITY SETTINGS will be properly protected
or specified.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data
sets that contain operating system components, MVS data sets that contain HFS
file systems with operating system components, and MVS data sets that contain

HFS file systems with application system and user data. All of these MVS data
sets require definitions in the ACP to enforce desired access controls. In
addition, the UNIX permission bits must be properly set on the HFS directories
and files to enforce desired access controls.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECCD-1, ECCD-2

Check Content:
The Systems Programmer will ensure that the HFS user audit bits for each file
match
settings listed in the table A-22 entitled System File Security Settings in
Section 2.5.2.5.2.

Use Vanguard Unix File Manager option 14 and review all files listed in the
SYSTEM FILE SECURITY SETTINGS Table in the U_zOS_STIG_Addendum:

NOTE: Some of the files listed in the referenced Z/OS STIG table are not used in
every
domain. If the file does not exist, there is NO FINDING.

a) If the HFS permission bits for each file match or are more restrictive than
the
specified settings listed in SYSTEM FILE SECURITY SETTINGS Table in the z/OS
STIG Addendum, there is NO 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)

b) If the HFS user audit bits for each file match or include the specified
settings listed SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum,

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

c) If (b) or (c) above is untrue, this is a FINDING.

Fix Text: The IAO with the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS 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-223849
Group Title: US000120
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000120
Rule Title: z/OS UNIX MVS data sets used as step libraries in /etc/steplib are not properly protected

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

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

Check Content:
The IAO will ensure that update and allocate access to libraries residing in the /etc/steplib is limited to system programmers only, unless a letter justifying access is filed with the IAO, all update and allocate access is logged.

a) Use Vanguard UNIX file manager option 14. Use the CD command to change to the /etc directory and use the browse command to review file located in

/etc/steplib

b) The RACF data set rules for libraries specified in the STEPLIBLIST file allow
inappropriate (e.g., global READ) access.

c) The RACF data set rules for libraries specified in the STEPLIBLIST file do
not
restrict UPDATE and/or ALTER access to only systems programming personnel.

d) The RACF data set rules for libraries specified in the STEPLIBLIST file do
not
specify that all (i.e., failures and successes) UPDATE and/or ALTER access will
be logged.

e) If all of the above are untrue, there is NO FINDING.

f) 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-223850
Group Title: US000130
Rule ID: N/A
Severity: CAT II

Rule Version (STIG-ID): US000130
Rule Title: The RACF Classes required to properly security the z/OS UNIX environment are not ACTIVE.

Vulnerability Discussion: The FACILITY, SURROGAT, and UNIXPRIV Class support
profiles used to secure the z/OS UNIX (OMVS) environment. Without these classes
being in an ACTIVE status, system integrity can be compromised.

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

Check Content:

The IAO will ensure that the ACTIVE CLASSES list includes entries for the FACILITY,
SURROGAT, and UNIXPRIV resource classes.

a) Review Vanguard Analyzer RACF Class Descriptor Table Analysis option 3; 1

b) Ensure the following CLASSES list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes are listed as STATUS is ACTIVE, there is NO FINDING.

c) If (b) above is untrue, this is a FINDING.

Fix Text:
UNIXPRIV class profiles are used to manage certain system privileges that are
typically associated with z/OS UNIX superuser authority. By defining UNIXPRIV
class profiles,
certain individual superuser privileges can be granted to users who do not have
superuser authority. This reduces the security risks associated with assigning
full superuser authority to users.

SURROGAT class profiles are only needed if there are servers (e.g., web server)
running in the z/OS UNIX environment that must be able to act with the security
context of a client and that client does not supply a password or other authenticator for the ACP.

FACILITY class profiles are used by a variety of IBM components including UNIX

System Services (OMVS). BPX prefixed profiles in this class are critical to the
proper security of the z/OS UNIX environment.

Ensure that the required classes are active. Develop a plan of action and activate with the RACF commands:

SETR CLASSACT(FACILITY SURROGAT UNIXPRIV)

SETR GENERIC(FACILITY SURROGAT UNIXPRIV)
SETR GENCMD(FACILITY SURROGAT UNIXPRIV)

SETR RACL(FACILITY SURROGAT UNIXPRIV)

CCI: CCI

CCI: CCI-002233

Group ID (Vulid): V-223851
Group Title: US000140
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000140
Rule Title: z/OS UNIX OMVS parameters in PARMLIB are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values
for z/OS UNIX security controls. The parameters impact HFS data access and
operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of
some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The Systems Programmer will ensure parmlib member IEASYSxx specifies parameter
OMVS and does not specify OMVS=DEFAULT.

a) Using Vanguard Analyzer online display select Parmlib Analysis option 3;L.
When Parmlib options are displayed press enter to continue. When the Parmlib
member list is presented locate the IEASYSxx member and browse this member.

NOTE: If the OMVS statement is not specified, OMVS=DEFAULT is used. This will result (as of Z/OS Release 2.8) in the Z/OS UNIX kernel starting in minimum
configuration mode. In minimum mode there is no access to permanent file systems
or to the shell, and IBM s Communication Server TCP/IP will not run.

b) If the parameter is specified as OMVS=xx or OMVS=(xx,xx,) in the IEASYSxx
member, there is NO FINDING.

c) If the parameter is not specified as OMVS=xx or OMVS=(xx,xx,), this is a
FINDING.

Fix Text: Review the settings in PARMLIB and /etc for z/OS UNIX security parameters and ensure that the values conform to the specifications below:

The parameter is specified as OMVS=xx or OMVS=(xx,xx,) in the IEASYSxx member.

NOTE: If the OMVS statement is not specified, OMVS=DEFAULT is used. In
minimum mode there is no access to permanent file systems or to the shell, and
IBM s Communication Server TCP/IP will not run.

CCI: CCI-000366

Group ID (Vulid): V-223852
Group Title: US000150
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000150
Rule Title: z/OS UNIX BPXPRMxx security parameters in PARMLIB are not properly
specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values
for z/OS UNIX security controls. The parameters impact HFS data access and
operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of
some system services.

Documentable: YES
Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The Systems Programmer will ensure parmlib member BPXPRMxx follows the specifications specified for the above control parameters SUPERUSER, STEPLIBLIST,
USERIDALIASTABLE, STARTUP_PROC, and MOUNT.

a) Use Vanguard Analyzer Parmlib Analysis option L. Browse all the BPXPRMxx
members.

b) Review the logical parmlib data sets, example: SYS1.PARMLIB(BPXPRMxx), for the following UNIX Parameter Keywords and Values:

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST (optional) /etc/steplib
If specified will use the above value.
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID or (SETUID (for Vendor-provided files)) &
 SECURITY (Specified regardless of Vendor-provided or not)
STARTUP_PROC OMVS

c) If the required parameter keywords and values are defined, there is NO FINDING.

d) If the required parameter keywords and values are not defined, this is a
FINDING.

Fix Text: Review the settings in PARMLIB member BPXPRMxx for z/OS UNIX security
parameters and ensure that the values conform to the specifications below:
Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUIDSETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS

BPXPRMxx is the SYS1.PARMLIB member that contains the parameters that control
the z/OS UNIX environment. BPXPRMxx controls the way features work and it establishes logical access to data by configuring the HFS environment.

The SUPERUSER parameter specifies the userid to be assigned to users when the su

command is entered without a userid operand. The userid must be defined to the
ACP as BPXROOT and have a UID of 0.

The TTYGROUP parameter specifies the group name assigned to pseudo terminals
(PTYs) and remote terminals (RTYs). The group must be defined to the ACP with a
unique GID and users must not be assigned to this group. This group name is used
by some shell commands (e.g., talk and write) when writing to the PTY or RTY
being used by another user. The name TTY must be used.

The STEPLIBLIST parameter specifies the pathname of the HFS file that contains
the list of MVS data sets that are used as step libraries for programs that have
the set-user-id or set group id permission bit set. The use of STEPLIBLIST is at
the site s discretion, but if used the value of STEPLIBLIST will be
/etc/steplib. All update and alter access to the MVS data sets in the list will
be logged and only systems programming personnel will be authorized to update
the data sets.

The USERIDALIASTABLE parameter specifies the pathname of the HFS file that
contains a list of userids and group names with their corresponding alias names.
The alias table is intended primarily for use where mixed or lower case userids
are used in the UNIX environment. Because the z/OS/ MVS components support only
upper case userids, the USERIDALIASTABLE will not be used.

The ROOT parameter specifies data for the file system that is to be mounted as
the root file system for z/OS UNIX. ROOT can have a number of sub-parameters;
the FILESYSTEM and SETUID|NOSETUID sub-parameters have security considerations.
FILESYSTEM can be used to specify the name of the MVS HFS data set that holds
the root file system. As the highest point in the HFS hierarchy, this file
system is critical to system operations. Therefore appropriate ACP access rules
must be written to protect the named data set. Update and alter access must be
restricted to the z/OS UNIX kernel and individual systems programming personnel.

The SETUID|NOSETUID sub-parameter specifies whether or not the set-user-ID or
set-group-ID permission bits are supported. SETUID|NOSETUID also impacts the APF
authorized and program-controlled extended attributes. For the root file system,
SETUID must be specified for normal operations.

The MOUNT parameter specifies data for a file system that is to be mounted by
z/OS UNIX. There are usually multiple MOUNT statements and each can have a
number of sub-parameters. The FILESYSTEM, SETUID|NOSETUID, and
SECURITY|NOSECURITY sub-parameters have significant security considerations.
FILESYSTEM can be used to specify the name of the MVS HFS data set that holds
the logical file system. Appropriate ACP access rules must be written to protect
the named data set. Update and alter access must be restricted to the z/OS UNIX
kernel and to individual systems programming personnel. The SETUID|NOSETUID sub
parameter specifies whether or not the set-user-ID or set group ID permission
bits are supported. SETUID|NOSETUID also impacts the APF authorized and
program-controlled extended attributes. SETUID may be specified for those file
systems that contain only vendor-provided software or that have been documented
to the IAO as requiring this support. Otherwise NOSETUID must be specified. The
SECURITY|NOSECURITY sub-parameter specifies whether security checks are
performed. SECURITY must be specified unless a specific exception for the file
system has been identified and documented to the IAO. Regardless of IBM
defaults, the values for SETUID|NOSETUID and SECURITY|NOSECURITY must be
explicitly coded to protect against potential vendor changes and to simplify
security reviews.

The STARTUP_PROC parameter specifies the name of the JCL procedure (PROC) that
starts the z/OS UNIX component. This started task must be defined to the ACP.
The name OMVS must be used.

CCI: CCI-000366

Group ID (Vulid): V-223853
Group Title: US000160
Rule ID: N/A
Severity: CAT II

Rule Version (STIG-ID): US000160
Rule Title: The z/OS Default profiles must not be defined in the corresponding
FACILITY Class Profile for classified systems.

Vulnerability Discussion: The RACF FACILITY Class BPX. UNIQUE.USER profile
contains the userid or the userid/group ID of the default profiles to be used
for a user without a z/OS UNIX profile (i.e., OMVS Segment). In classified
system user access will not be determined by default.

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

Check Content:
The IAO will ensure that the BPX.DEFAULT.USER for the FACILITY resource class is
only used for FTP socket applications on non classified systems.

If the system is not classified this is not applicable.

a) Review System Classification General Resource Profile BPX.DEFAULT.USER
Using Vanguard Administrator General Resource Reports option 3;4 Mask on
Profile=BPX.DEFAULT.USER and class=FACILITY.

b) If system is classified or does not use the FTP socket application the Default User
and Default Group are not defined in the Application Data field in the
BPX.DEFAULT.USER resource in the FACLILITY report, there is NO
FINDING.

c) If the system is a non classified system, running the FTP socket application,
and
has Default User and Default Group defined in the Application Data field in the
BPX.DEFAULT.USER resource in the FACLILITY report, there is NO
FINDING.

d) If (b) and (c) above are untrue, this is a FINDING.

Fix Text: 1. If system is classified a userid should not be defined in the
application data field of the FACILITY report.

The sample commands below show the required security parameters required for the
default user:

```
AG OEDFLTG SUPGROUP(ADMIN) OWNER(ADMIN) OMVS(GID(777777))

AU OEDFLTU DFLTGRP(OEDFLTG) NAME('OE DEFAULT USER') NOPASS -
 OMVS(UID(99999) HOME('/u/oeflt') PROGRAM('/bin/echo')) -
 DATA('DEFAULT OMVSUSERID ADDED WITH SOER5')


RDEF FACILITY BPX.DEFAULT.USER APPLDATA('OEDFLTU/OEDFLTG') -
 DATA('ADDED TO SUPPORT THE DEFAULT USER') UACC(NONE) OWNER(ADMIN)

SETR RACLIST(FACILITY) REFRESH
```

CCI: CCI-000366

Group ID (Vulid): V-223854
Group Title: US000170
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000170
Rule Title: z/OS UNIX HFS MapName files security parameters are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The Systems Programmer will ensure that if the /etc/auto.master HFS FILE is used that each /etc/mapname file listed specifies setuid no and security yes, unless a letter justifying a specific exception is filed with the IAO.

a) Use Vanguard Analyzer option 3-Online Displays, Parmlib Analysis option L.
Browse the BPXPRMxx members

b) Review the logical 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.

NOTE: The /etc/auto.master HFS file (and the use of Automount) is optional.
If the file does not exist, this is NOT APPLICABLE.

NOTE: The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified
and not allowed to default.

c) If each MapName file specifies the setuid No and security Yes statements for
each automounted directory, there is NO FINDING.

d) If there is a deviation from the required values and documentation for the
deviation exists, there is NO FINDING.

NOTE: security No disables security checking for file access. Security No is
only allowed on test and development domains. setuid Yes allows a user to run
under a different UID/GID identity. Justification documentation is required to
validate the use of setuid Yes.

e) If (c), or (d) above is untrue, this is a FINDING.

Fix Text: Review the settings in /etc/auto.master and /etc/mapname for z/OS UNIX
security parameters and ensure that the values conform to the specifications
below.

The /etc/auto.master HFS file (and the use of Automount) is optional.
The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified
and not be allowed to default.

Each MapName file will specify the setuid NO and security YES statements for
each automounted directory

If there is a deviation from the required values, documentation must exist for
the deviation.

Security NO disables security checking for file access. Security NO is only

allowed on test and development domains.

Setuid YES allows a user to run under a different UID/GID identity. Justification documentation is required to validate the use of setuid YES.

CCI: CCI-001762

Group ID (Vulid): V-223855
Group Title: US000180
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000180
Rule Title: z/OS UNIX security parameters for restricted network service(s) in
/etc/inetd.conf are not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values
for z/OS UNIX security controls. The parameters impact HFS data access and
operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of
some system services.

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

Check Content:
The Systems Programmer or IAO will ensure that the restricted network services
specified
in the /etc/inetd.conf file listed in the table below are disabled, unless a
letter justifying the
use of the restricted network service is on file with the IAO.
RESTRICTED NETWORK SERVICES

Service	Port
Chargen	19
Daytime	13
Discard	9
Echo	7
Exec	512
finger	79
shell	514
time	37
login	513
smtp	25
timed	525

```
nameserver              42
systat                    11
uucp                    540
netstat                    15
talk                    517
qotd                    17
tftp                    69
```

a) Using Vanguard Administrator UNIX file manager option 14. Use the CD command to change to /etc directory and browse the inetd.conf file.

b) If all the services in the table above are not found in or are commented out
of the
/etc/inetd.conf file, there is NO FINDING.

c) If any of the Restricted Network Services defined above is specified, this is
a
FINDING.

Fix Text: Review the settings in The /etc/inetd.conf file determine if every
entry in the file represents a service that is actually in use. Services that
are not in use must be disabled to reduce potential security exposures.
The following services must be disabled in /etc/inetd.conf unless justified and
documented with the IAO:

RESTRICTED NETWORK SERVICES

```
Service                    Port
Chargen                    19
Daytime                    13
Discard                    9
Echo                    7
Exec                    512
finger                    79
shell                    514
time                    37
login                    513
smtp                    25
timed                    525
nameserver              42
systat                    11
uucp                    540
netstat                    15
talk                    517
qotd                    17
```

tftp 69

/etc/inetd.conf
The /etc/inetd.conf file is used by the INETD daemon. It specifies how INETD is
to handle service requests on network sockets. Specifically, there is one entry
in inetd.conf for each service. Each service entry specifies several parameters.
The login_name parameter is of special interest. It specifies the userid under
which the forked daemon is to execute. This userid is defined to the ACP and it
may require a UID(0) (i.e., superuser authority) value.

CCI: CCI-000382

CCI: CCI-001762

Group ID (Vulid): V-223856
Group Title: US000190
Rule ID: N/A
Severity: CAT I
Rule Version (STIG-ID): US000190
Rule Title: UID(0) is improperly assigned.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and
Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are
defined to an ACP with attributes including UID and GID. If these attributes are
not correctly defined, data access or command privilege controls could be compromised.

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

Check Content:
The Systems Programmer and IAO will ensure that UID(0) is assigned only to
system
tasks such as the Z/OS UNIX kernel (i.e., OMVS or OMVSKERN), Z/OS UNIX
daemons (e.g., inetd, syslogd, ftpd), and other system software daemons; 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.

a) Review Vanguard Administrator User OMVS Segment Report option 3;5;9 Mask
on UID =0

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. As discussed in the Z/OS STIG, 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-223857
Group Title: US000200
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000200
Rule Title: Attributes of z/OS UNIX user accounts are not defined properly

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
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.a)

a) Review Vanguard Administrator Group OMVS Segment report 3;5;22

NOTE: A site can choose to have both an OMVSGRP group and an STCOMVS group or combine the groups under one of these names.

b) If the OMVSGRP group and / or the STCOMVS group are each defined with a unique GID in the range of 1-99, there is NO FINDING.

c) If (b) above is untrue, this is a FINDING.

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-223859
Group Title: US000220
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000220
Rule Title: The user account for the z/OS UNIX kernel (OMVS) is not properly
defined to the security database.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and
Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are
defined to an ACP with attributes including UID and GID. If these attributes are
not correctly defined, data access or command privilege controls could be compromised.

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

Check Content:

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-223860
Group Title: US000230
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000230
Rule Title: The user account for the z/OS UNIX SUPERUSER userid must be properly
defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and
Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are
defined to an ACP with attributes including UID and GID. If these attributes are
not correctly defined, data access or command privilege controls could be compromised.

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

Check Content:
___STIG ID: ZUSS0045 Default Severity: Category II

The Systems Programmer and IAO will ensure that the RMFGAT user account is
properly defined in the security database.
RMFGAT is the userid for the Resource Measurement Facility (RMF) Monitor III
Gatherer. If RMFGAT is not defined this is not applicable.

a) Review Administrator User OMVS Segment Report 3;5;9 Mask on

USERID=RMFGAT

b) Enter an LV next to the UserID to display the user information. The default group will be located under GENERAL INFORMATION; the remainder of the information will be located under OMVS SEGMENT.

c) If RMFGAT is defined as follows, there is NO FINDING:
1. Default group specified as OMVSGRP or STCOMVS
2. A unique, non-zero UID
3. HOME directory specified as /
4. Shell program specified as /bin/sh

d) If RMFGAT is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

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-223861
Group Title: US000240
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000240
Rule Title: The user account for the z/OS UNIX (RMFGAT) is not properly defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

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

Check Content:
___STIG ID: ZUSS0044 Default Severity: Category II

The user account for the z/OS UNIX SUPERUSER userid must be properly defined.

a) Review Vanguard Administrator USER OMVS Segment Report 3;5;9 Mask on
USERID=BPXROOT
b) Refer to system PARMLIB member BPXPRMxx (xx is determined by OMVS entry
in IEASYS00.)

c) If BPXROOT 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

d) If BPXROOT is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

Fix Text: Define the RMFGAT user account as specified below:

- Default group specified as OMVSGRP or STCOMVS
- A unique, non-zero UID
- HOME directory specified as /
- Shell program specified as /bin/sh

CCI: CCI-000764

Group ID (Vulid): V-223862
Group Title: US000250
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000250
Rule Title: z/OS UNIX user accounts are not properly defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and
Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are
defined to an ACP with attributes including UID and GID. If these attributes are

not correctly defined, data access or command privilege controls could be compromised.

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

Check Content:
The Systems Programmer and IAO will ensure that each user account is defined
with a
unique UID number (except for UID(0) users), a unique HOME directory (except for
UID(0) and other system task accounts), and shell program specified as "/bin/sh",
"/bin/tcsh", or "/bin/false."

a) Review Vanguard Administrator USER OMVS SEGMENT report option 3;5;9. Sort by UID.
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-223863
Group Title: US000260
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): US000260
Rule Title: Attributes of z/OS UNIX user accounts used for account modeling must
be defined in accordance with security requirements.

Vulnerability Discussion: RACF userids that use z/OS UNIX must be properly
configured. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:
The Systems Programmer and IAO will ensure that the below bulleted options are
enforced for FTP socket applications using shared OMVS segments.

* Application of the APAR PQ63326 to control FTP access to UNIX files is required.
* Collection of SMF type 80 records to track user access to OMVS default UID.
* Use of the OMVS default UID will not be allowed on any classified system.
* The definition of the OMVS default user will be restricted to a non-0 UID, a
non-
writable home directory, such as "\" root, and a non-executable, but existing,
binary file,"/bin/false" or "/bin/echo."

NOTE: This check only applies to the OMVS default user. If the OMVS default user
is not defined in the Application Data field in the BPX.DEFAULT.USER resource in
the FACILITY report, this is NOT APPLICABLE.

a) Using Vanguard Administrator General Resource Profile report mask on Profile=BPX.DEFAULT.USER and Class=facility. . Use the LV command to review this profile document the APPL Data I.E. USERID/GROUPID for later use.

b) Repeat step a), masking on Profile=BPX.UNIQUE.USER.

c) Using Vanguard Administrator User Report mask on USER id=USERID (the OMVS default user) documented above. Use the VRC command to view the user profile. Find the OMVS Segment Information and review. If OMVS default user
account is defined as follows, there is NO FINDING.
1. A non-writable HOME directory
2. Shell program specified as /bin/echo , or /bin/false

d) Repeat step c), masking on USER id=USERID (the OMVS unique user) documented
above in step b). If OMVS unique user account is defined as follows, there is NO
FINDING.
1. A non-writable HOME directory
2. 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).

e) If the user account is not defined as specified in (b) above, this is a FIND

Fix Text: Use of the OMVS default UID will not be allowed on any classified
system. This is not an issue when using BPX.UNIQUE.USER.

Define user id used for OMVS account modeling with a non-0 UID, a non-writable
home directory, such as "\" root, and a non-executable, but existing, binary
file, "/bin/false" or /bin/echo.

```
AG OEDFLTG SUPGROUP(ADMIN) OWNER(ADMIN) OMVS(GID(777777))
AU OEDFLTU DFLTGRP(OEDFLTG) NAME('OE DEFAULT USER') NOPASS -
OMVS(UID(99999) HOME('/u/oeflt') PROGRAM('/bin/echo')) -
DATA('DEFAULT OMVSUSERID ADDED WITH SOER5')
RDEF FACILITY BPX.DEFAULT.USER APPLDATA('OEDFLTU/OEDFLTG') -
DATA('ADDED TO SUPPORT THE DEFAULT USER') UACC(NONE) OWNER(ADMIN)
SETR RACLIST(FACILITY) REFRESH
```

CCI: CCI-000764

Group ID (Vulid): V-223864
Group Title: UT000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): UT000010
Rule Title: The startup user account for the z/OS UNIX Telnet Server is not
defined properly.

Vulnerability Discussion: The z/OS UNIX Telnet Server (i.e., otelnetd) requires
a UID(0) to provide its system services. After the user enters their userid and
password, otelnetd switches to the security context of the users account. Because the otelnetd account is only used until authentication is completed,
there is no need to require a unique account for this function. This limits the
number of privileged accounts defined to the ACP and reduces the exposure potential. Failure to properly define and control otelnetd could lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
startup user
account for otelnetd is the account defined for the Z/OS UNIX kernel.

a) Using Vanguard Administrator UNIX File Manger option 14 use the CD command to change to the /etc directory and the browse command to review /etd/inetd.conf file.

```
#==============================================================
# service | sock | prot | wait/ | user | server | server program
# name | type | | nowait | | program | arguments
#==============================================================
otelnet stream tcp nowait OMVSKERN /usr/sbin/otelnetd otelnetd m
```

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

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-223865
Group Title: UT000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): UT000020
Rule Title: HFS objects for the z/OS UNIX Telnet Server will be properly protected.

Vulnerability Discussion: HFS directories and files of the z/OS UNIX Telnet
Server provide the configuration and executable properties of this product.
Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating
system environment, ACP, and customer data.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
permission
bits and user audit bits for HFS objects that are part of the Z/OS UNIX Telnet
Server
component is configured according to the settings in the following table:

z/OS UNIX TELNET SERVER HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION BITS	USER AUDIT BITS
/usr/sbin/otelnetd	1740	fff
/etc/banner	0744	faf

a) Using Vanguard Administrator UNIX file manager option 14 open files browse
files above and review Permission bits and USER Audit bits.

b) If the HFS permission bits and user audit bits for each directory and file
match or
are more restrictive than the specified settings listed in the table above,
there is
NO FINDING.

NOTE: The /usr/sbin/otelnetd object is a symbolic link to
/usr/lpp/tcpip/sbin/otelnetd.
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

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

Fix Text: The IAO with the assistance of a systems programmer with UID(0)
and/or
SUPERUSER access, will review the UNIX permission bits and user audit
bits on
the HFS directories and files for the 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/otelnetd	1740	fff
/etc/banner	0744	faf

NOTE:
The /usr/sbin/otelnetd object is a symbolic link to
/usr/lpp/tcpip/sbin/otelnetd. 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/otelnetd
chaudit rwx=f /usr/lpp/tcpip/sbin/otelnetd
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-223866
Group Title: UT000030
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): UT000030
Rule Title: The warning banner for the z/OS UNIX Telnet Server is not specified
or not properly specified.

Vulnerability Discussion: A logon banner can be used to inform users about the
environment during the initial logon. Logon banners are used to warn users
against unauthorized entry and the possibility of legal action for unauthorized
users, and advise all users that system use constitutes consent to monitoring.
Failure to display a logon warning banner without this type of information could
adversely impact the ability to prosecute unauthorized users and users who abuse
the system.

Documentable: YES
Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, ECWM-1

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
otelnetd
startup command includes the options -D login and -c 900, where:
-D login indicates that messages should be written to the syslogd facility for
login
and logout activity
-c 900 indicates that the Telnet session should be terminated after 15 minutes
of
inactivity.

The systems programmer responsible for supporting ICS will ensure that the
otelnetd
startup command does not include the option -h, where:
-h indicates that the logon banner should not be displayed.

a) Using Vanguard Administrator UNIX File Manager option 14. User the CD command to change to the etc directory and the browse the file /etc/inetd.conf

b) Ensure the following items are in effect for the otelnetd startup command:
1. Option -D login is included on the otelnetd command.
2. Option -c 900 is included on the otelnetd command.

NOTE: 900 indicates a session timeout value of 15 minutes and is currently the
maximum value allowed.

3. Option -h is not included on the otelnetd command.

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

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

Fix Text: Review the /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-223867
Group Title: UT000040
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): UT000040
Rule Title: Startup parameters for the z/OS UNIX Telnet Server are not specified
properly.

Vulnerability Discussion: The z/OS UNIX Telnet Server (i.e., otelnetd) provides
interactive access to the z/OS UNIX shell. During the initialization process,
startup parameters are read to define the characteristics of each otelnetd
instance. Some of these parameters have an impact on system security. Failure to
specify the appropriate command options could result in degraded security. This
exposure may result in unauthorized access impacting data integrity or the
availability of some system services.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:
The systems programmer responsible for supporting ICS will ensure that the
otelnetd
startup command includes the options -D login and -c 900, where:
-D login indicates that messages should be written to the syslogd facility for
login
and logout activity

-c 900 indicates that the Telnet session should be terminated after 15 minutes
of
inactivity.

The systems programmer responsible for supporting ICS will ensure that the
otelnetd
startup command does not include the option -h, where:
 -h indicates that the logon banner should not be displayed.

a) Using Vanguard Administrator UNIX File Manager option 14. User the CD command to change to the etc directory and the browse the file /etc/inetd.conf

b) Ensure the following items are in effect for the otelnetd startup command:
1. Option -D login is included on the otelnetd command.
2. Option -c 900 is included on the otelnetd command.

NOTE: 900 indicates a session timeout value of 15 minutes and is currently the
maximum value allowed.

If Option -D login is included on the otelnetd command, this is not a finding.

If Option -c 900 is included on the otelnetd command, this is not a finding.

NOTE: "900" indicates a session timeout value of "15" minutes and is currently
the maximum value allowed.

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-000366

Group ID (Vulid): V-223868
Group Title: UT000050
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): UT000050
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.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Check Content:

The systems programmer responsible for supporting ICS will ensure that the
otelnetd
startup command includes the options -D login and -c 900, where:
-D login indicates that messages should be written to the syslogd facility for
login
and logout activity
-c 900 indicates that the Telnet session should be terminated after 15 minutes
of
inactivity.

The systems programmer responsible for supporting ICS will ensure that the
otelnetd
startup command does not include the option -h, where:
-h indicates that the logon banner should not be displayed.

a) Using Vanguard Administrator UNIX File Manager option 14. User the CD

command to change to the etc directory and the browse the file /etc/inetd.conf

b) Ensure the following items are in effect for the otelnetd startup command:
1. Option -D login is included on the otelnetd command.
2. Option -c 900 is included on the otelnetd command.

NOTE: 900 indicates a session timeout value of 15 minutes and is currently the
maximum value allowed.

3. Option -h is not included on the otelnetd command.
Enter /etc/ for a pathname - you may need to issue a CD /etc/
select FILE NAME inetd.conf

If Option -h is included on the otelnetd command, this is a finding.
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

CCI: CCI-001384CCI

CCI: CCI-001385CCI

CCI: CCI-001386CCI

CCI: CCI-001387CCI

CCI: CCI-001388

Group ID (Vulid): V-223869
Group Title: VT000010
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): VT000010
Rule Title: The System datasets used to support the VTAM network are not properly secured.

Vulnerability Discussion: Ensure that RACF 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.

Failure to properly control VTAM datasets could potentially compromise the
network operations.

Responsibility: Systems Programmer
IAControls: N/A

Check Content:
a) Refer to the following item gathered from the VTAM Systems Programmer s
Worksheet in the Preliminary Information
Worksheets(U_zOS_STIG_INSTRUCTION.doc):

___ 1. 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 environments.

b) Generate a report for security verification using Analyzer.
1. Select option 4 Batch Reports from the Analyzer main menu
2. Select option B Sensitive and Critical Data Sets Analysis
3. Enter R on line item User defined list
4. Provide a dataset name or your choice which will include the names of the
data sets gathered from step a) above.

Note: This may be a sequential data set or a PDS and member

5. Specify the options as listed here.

AC(1) module list ===NO Duplicate Module Analysis ===NO
RACF detail ===YES Exceptions only ===NO
RACF Group detail ===YES
Search criteria ===NO
Sort criteria ===NO

6. Press enter to invoke the JCL Submit Processing
7. Enter S to submit the batch report
8. Review the report for findings

b) Ensure that RACF 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 (c) above is true, there is NO FINDING.

d) If (c) above is untrue, this is a FINDING.

Fix Text: Data Set Controls

Ensure that RACF 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 RACF commands show proper definitions/permissions for VTAM
datasets:

```
AD 'SYS1.VTAM*.**' UACC(NONE) OWNER(SYS1) -
 AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -
 DATA('IBM VTAM DS PROFILE: REF SRR PDI ZVTM0018')
PE 'SYS1.VTAM.**' ID(<syspaudt>) ACC(A)

AD 'SYS1.VTAMLIB.**' UACC(NONE) OWNER(SYS1) -
 AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -
 DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')
PE 'SYS1.VTAMLIB.**' ID(<syspaudt>) ACC(A)

AD 'SYS1.VTAM.SISTCLIB.**' UACC(NONE) OWNER(SYS1) -
 AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -
 DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')
PE 'SYS1.VTAM.SISTCLIB.**' ID(<syspaudt>) ACC(A)
```

```
 AD 'SYS3.VTAM.**' UACC(NONE) OWNER(SYS3) -
 AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -
 DATA('VTAM CUSTOMIZED DS: REF SRR PDI ZVTM0018')
 PE 'SYS3.VTAM.**' ID(<syspaudt>) ACC(A)

 AD 'SYS3.VTAMLIB.**' UACC(NONE) OWNER(SYS3) -
 AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -
 DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')
 PE 'SYS3.VTAMLIB.**' ID(<syspaudt>) ACC(A)

 SETR GENERIC(DATASET) REFRESH
```

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223870
Group Title: VT000020
Rule ID: N/A
Severity: CAT II
Rule Version (STIG-ID): VT000020
Rule Title: The VTAM USSTAB definitions are being used for unsecured terminals

Vulnerability Discussion: VTAM options and definitions are used to define VTAM operational capabilities. They must be strictly controlled. Unauthorized users could override or change start options or network definitions. Failure to properly control VTAM resources could potentially compromise the network operations.

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

Check Content:
a) Refer to the following items gathered from the VTAM Systems Programmers Worksheet in the Preliminary Information Worksheets in U_zOS_STIG_INSTRUCTION.doc:

___ 1. Documentation regarding terminal naming standards.

___ 2. Documentation of all procedures controlling terminal logons to the system.

___ 3. A complete list of all USS commands used by terminal users to log on to the system.

___ 4. A complete list of all terminals and/or terminal types controlled by
LOGAPPL definitions only.

___ 5. Members and data set names containing USSTAB and LOGAPPL definitions of all terminals that can log on to the system (e.g., SYS1.VTAMLST).

___ 6. Members and data set names containing logon mode parameters.

b) If USSTAB definitions are only used for secure terminals (e.g., terminals
that are
locally attached to the host or connected to the host via secure leased lines),
there
is NO FINDING.

Fix Text: The Systems programmer and IAO will verify that USSTAB definitions are
only used for secure terminals.

Only terminals that are locally attached to the host or connected to the host
via secure leased lines located in a secured area. Only authorized personnel may
enter the area where secure terminals are located.

USSTAB or LOGAPPL definitions are used to control logon from secure terminals.
These terminals can log on directly to any VTAM application (e.g., TSO, CICS,
etc.) of their choice and bypass Session Manager services. Secure terminals are
usually locally attached to the host or connected to the host via a private LAN
without access to an external network. Only authorized personnel may enter the
area where secure terminals are located.

CCI: CCI-001499

UNCLASSIFIED