UNCLASSIFIED

z/OS RACF STIG

Version: 7

Release: 1

15 Mar 2025

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

_____

Group ID (Vulid): V-224483
Group Title: ZFEP0011
Rule ID: SV-7195r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZFEP0011
Rule Title: All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

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

Check Content:
a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 1, in the
Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):
* Item 1: Documents and procedures restricting access to the hardware
components of the FEPs.

b) If the hardware components of the FEPs are located in secure locations, there is
NO FINDING.

c) If the hardware components of the FEPs are not located in secure locations, this is
a FINDING.

Fix Text: Ensure that hardware components of the FEPs are protected as specified below:

Physical security is the first level of security control for the FEPs. Install all hardware components of the FEPs in secure locations where they cannot be stolen, damaged, or disturbed. Make sure that FEP hardware is located in a secure area with limited access to authorized personnel.

CCI: CCI-000933

_____

Group ID (Vulid): V-6901
Group Title: ZFEP0012
Rule ID: SV-7196r2_rule

Severity: CAT II
Rule Version (STIG-ID): ZFEP0012
Rule Title: Procedures are not in place to restrict access to FEP functions of the service subsystem from operator consoles (local and/or remote), and to restrict access to the diskette drive of the service subsystem.

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

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

Check Content:
a) Refer to the Front End Processor (FEP) Protection Worksheet, Items 1-4, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

* Item 1: Documents and procedures restricting access to the hardware components of the FEPs.
* Item 2: Documents and procedures restricting access to the functions of the service subsystem from the control panel.
* Item 3: Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).
* Item 4: Documents and procedures restricting access to the diskette drive of the service subsystem.

b) If a procedure is in place to restrict access to the functions of the service subsystem, there is NO FINDING.

c) If a procedure is in place to restrict access to the functions of the service subsystem from operator consoles (local and/or remote), there is NO FINDING.

d) If a procedure is in place to restrict access to the diskette drive of the service subsystem, there is NO FINDING.

e) If no procedure exists for any of the above functions of the service subsystem and FEP resources, this is a FINDING.

Fix Text: Ensure that all hardware components of the FEPs are protected as decribed below and supporting documentation procedures exist for each item:

1. Documents and procedures restricting access to the hardware components of the FEPs.

2. Documents and procedures restricting access to the functions of the service subsystem from the control panel.

3. Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).

4. Documents and procedures restricting access to the diskette drive of the service subsystem.

CCI: CCI-000004

_____

Group ID (Vulid): V-224485
Group Title: ZFEP0013
Rule ID: SV-7197r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZFEP0013
Rule Title: A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program).

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

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

Check Content:
a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 6, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):
* Item 6: Documents and procedures regarding the NCP load and dump processes.

b) If a procedure is in place relative to the NCP load and dump processes, there is NO FINDING.

c) If no procedure is in place relative to the NCP load and dump processes, this is a FINDING.

Fix Text: If documented procedures for loading and dumping the FEP NCP (Network Control Program) are not available. Create a procedure document for dumping and loading the FEP and make sure that they are available to the IAO and to authorized personnel responsible to perform these functions.

CCI: CCI-000504

_____

Group ID (Vulid): V-224486
Group Title: ZFEP0014
Rule ID: SV-7198r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZFEP0014
Rule Title: An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor).

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

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

Check Content:
a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 8, in the
Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):
* Item 8: All documents and procedures that apply to FEP operations including
network management, FEP initialization, IPL, shutdown, NCP dumping,
backup, and recovery.

b) If a log is in place to keep track of all hardware upgrades and software changes,
there is NO FINDING..

c) If a log is in place to keep track of all hardware upgrades and software changes,
there is NO FINDING.

Fix Text: The systems programmer will see that a a log of all hardware and software upgrades/changes has been created for auditing purposes and problem tracking. All changes and upgrades will be logged.

CCI: CCI-000318

_____

Group ID (Vulid): V-224487
Group Title: ZFEP0015
Rule ID: SV-7199r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZFEP0015
Rule Title: NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE

and/or ALLOCATE access to appropriate personnel.

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

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

Check Content:
a) Reference data from item 4 of the Z/OS Systems Programmer s Worksheet, located in U_zOS_STIG_INSTRUCTION.doc to locate the JES2 proclibs.

b) Search the JES2 proclibs for the member that executes program ISTINM01. These data sets are used for the FEP at the site; if the domain does not have a FEP the collection of these data sets can be bypassed. Review the VTAM procedure for load and dump data sets for the FEP. Use ISPF/PDF option 3.4 data set name list to enter **.*NCP*. Enter the names of the above datasets in a sequential dataset. Make note of the dataset name for item C below.

c) From Analyzer main Menu, go to B, Sensitive Critical Data Sets Analysis , enter R to the left of User defined list . Enter the name of the sequential dataset created from above to the right of the ===>. Press enter.

d) Review the User defined list shown. If there are entries in the displayed list that have either R, N, E, or W in the M column, there is a FINDING for NCP data sets allowing inappropriate access.

e) Review each data set shown in the User defined list by entering VRC under the Opt heading. Check the access to these data set rules to ensure they do not allow UPDATE and/or ALTER access to authorized personnel (e.g., Z/OS systems programming personnel). If any allow UPDATE or ALTER access, this is a FINDING

Fix Text: Identify Names of the following data sets used for installation and in development/production environments:

- NCP system data sets
- NCP source definition data sets
- NCP load modules
- NCP host dump data sets
- NCP utility programs

Have the IAO validate that they are properly protected by the ACP. And that only authorized personnel are permitted UPDATE and/or ALLOCATE access (e.g., z/OS systems programming personnel).

CCI: CCI-001499

_____

Group ID (Vulid): V-224725
Group Title: ZFEP0016
Rule ID: SV-7200r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZFEP0016
Rule Title: A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem.

Vulnerability Discussion: If components of the FEPs are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the control panel, the operator console, and the diskette drive of the service subsystem. Therefore, they can interfere with the normal operations of the FEPs. Improper control of FEP components could compromise network operations.

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

Check Content:
a) Refer to the Front End Processor (FEP) Protection Worksheet, Items 1-4, in the Preliminary Information Worksheets (U_zOS_STIG_INSTRUCTION.doc):

* Item 1: Documents and procedures restricting access to the hardware components of the FEPs.
* Item 2: Documents and procedures restricting access to the functions of the service subsystem from the control panel.
* Item 3: Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).
* Item 4: Documents and procedures restricting access to the diskette drive of the service subsystem.
b) If a password control is in place to restrict access to the service subsystem via the operator consoles (local and/or remote), there is NO FINDING.

a) If a key-lock switch is used to protect the modem supporting the remote console of the service subsystem, there is NO FINDING.

b) If no procedure exists for any of the above functions of the service subsystem and FEP resources, this is a FINDING.

Fix Text: If any of the below procedures are not in place, than correct the situation by documenting the missing procedure(s).

The systems programmer should validate that Control authorization to use service subsystem console (local or remote) by FEP internal security control through password validation. Restrict access to these passwords to the absolutely minimum number of necessary personnel. Use of vendor default passwords is prohibited. Assign different passwords for the local and remote consoles. Disconnect the local/remote console after three unsuccessful attempts to log on. Passwords used by vendor (COMTEN, IBM, CNT, or AMDAHL) service personnel will be changed after any maintenance is done. All passwords will be changed every 90 days. Restrict permission to change passwords only to authorized personnel.

Use a key lock switch on the modem supporting the remote console of the service subsystem to prevent unauthorized access. The key lock switch is only open for scheduled and authorized remote access.

CCI: CCI-000213

_____

UNCLASSIFIED