z/OS NetView for RACF STIG

Version: 6

Release: 9

30 June 2023

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

---

Group ID (Vulid):  V-18014
Group Title:  ZB000040
Rule ID:  SV-28492r4_rule
Severity: CAT II
Rule Version (STIG-ID):  ZNET0040
Rule Title: NetView configuration/parameter values must be specified properly.

Vulnerability Discussion:  NetView configuration/parameters control the security
and operational characteristics of products. If these parameter values are
improperly specified, security and operational controls may be weakened. This
exposure may threaten the availability of the product applications, and

compromise the confidentiality of customer data.

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

Check Content:

The following steps are necessary for reviewing the NETVIEW options:

a) Review the member CxxSTYLE in the DSIPARM DD statement concatenation of the NetView CNMPROC STC procedure. (This member is located in SYS3.NETVIEW.DSIPARM.)

b) Verify that they are the same as the following specifications: Example

Keyword Value
SECOPTS.OPERSEC SAFCHECK|SAFDEF
SECOPTS.CMDAUTH SAF.FAIL/SAF.TABLE

c) If they are the same as specified in (b) this is not a finding.

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

Fix Text: The Systems Programmer and IAO will review NetView configuration parameters and control options for compliance.

To ensure authentication of users to NetView, ensure that CxxSTYLE in the DSIPARM DD statement concatenation of the NetView CNMPROC STC procedure has the following initialization parameter(s) specified:

(Note: The data set identified above is an example of a possible installation. The data set is determined when the product is actually installed on a system through the product s installation guide and can be site specific.)

SECOPTS.OPERSEC=SAFCHECK|SAFDEF

When SECOPTS.OPERSEC=SAFCHECK is used, it specifies that operator identification and password or password phrase checking is performed using an SAF security product. The operator identifier must also be defined in DSIOPF, and other attributes given to the operator at logon are taken from the specified profile for the operator in DSIPRF.

Security access checks are checked against the authority of the operator that occur when an operator tries to access a data set that is protected in the DATASET class of an SAF product or an MVS system command that is protected in the OPERCMDS class of an SAF product.

When SECOPTS.OPERSEC=SAFDEF is used, it specifies that operator identification and password or password phrase checking is done using an SAF security product. Authority to log on as a NetView operator is controlled through the APPL class. The operator identifier must be authorized to the resource name in the APPL class which represents the NetView program.

The attributes given to the operator at logon are defined in the NETVIEW segment of the user profile for the operator in the SAF product. For more information, refer to IBM Tivoli NetView for z/OS Security Reference.

When SECOPTS.OPERSEC=SAFDEF is specified, any value for SECOPTS.CMDAUTH can be used.

Additional details can be obtained in the IBM Tivoli NetView for z/OS Security Reference.

SECOPTS.CMDAUTH=SAF.FAIL|SAF.table

When SECOPTS.CMDAUTH=SAF.table is used, table specifies the backup table to be used for immediate commands and when the SAF product cannot make a security decision. This can occur when:

___ No resource name is defined in the NETCMDS class which protects or authorizes this command.
___ The NETCMDS class is not active.
___ The security product is not active.

When SECOPTS.CMDAUTH=SAF.FAIL is used, command authority checking will fail if the SAF product can reach no decision.

Additional details can be obtained in the IBM Tivoli NetView for z/OS Administration Reference.

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-27314r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETR000
Rule Title: NetView install data sets are not properly protected.

Vulnerability Discussion: NetView Install data sets provide the capability 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 CL/Supersession Installation Datasets, Likely:
1. hlq.NETVIEW.**
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 lower (READ is acceptable)
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
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.
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 NetView install data sets is limited to System Programmers only and all update and allocate access is logged. Auditors should be granted READ access.

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:
SYS2.NETVIEW
SYS2A.NETVIEW
SYS3.NETVIEW

```
ad 'sys2.netview.**' uacc(none) owner(sys2) -
audit(success(update) failures(read))
pe 'sys2.netview.**' id(syspaudt) acc(a)
pe 'sys2.netview.**' id(audtaudt)
ad 'sys2a.netview.**' uacc(none) owner(sys2a) -
audit(success(update) failures(read))
pe 'sys2a.netview.**' id(syspaudt) acc(a)
pe 'sys2a.netview.**' id(audtaudt)
ad 'sys3.netview.**' uacc(none) owner(sys3) -
audit(success(update) failures(read))
pe 'sys3.netview.**' id(syspaudt) acc(a)
pe 'sys3.netvidew.**' id(audtaudt)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-27322r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETR001
Rule Title: NetView STC data sets are not properly protected.

Vulnerability Discussion: NetView STC data sets provide the capability 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, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Check with your IOA or Systems Programming personnel and compile the list of
CL/Supersession STC datasets, Likely:
1. hlq.NETVIEW.<systemid>.**
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. 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, Product STC(s) and/or Batch Jobs and READ access is limited to
Auditors.
9. 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 is limited to Systems Programming personnel, Product
STC(s) and/or Batch Jobs and READ access is limited to Auditors.
10. 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 NetView STC
data sets are limited to System Programmers and NetView STC only, unless a
letter justifying access is filed with the IAO. Auditors should have READ access.

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 and/or alter 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:
SYS3.NETVIEW.<systemid>.** (VSAM data sets)

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

```
ad 'sys3.netview.<systemid>.<VSAMDS>.**' uacc(none) owner(sys3) -
audit(success(update) failures(read)) -
data('netview site VSAM datasets')
pe 'sys3.netview.<systemid>.**' id(audtaudt) acc(r)
pe 'sys3.netview.<systemid>.**' id(CNMPROC syspaudt tstcaudt) acc(a)
```

The VSAM Dataset required for greater than read access are:

```
SYS3.NETVIEW.<systemid>.AAUVSPL
SYS3.NETVIEW.<systemid>.AAUVSSL
SYS3.NETVIEW.<systemid>.BNJLGPR
SYS3.NETVIEW.<systemid>.BNJLGSE
SYS3.NETVIEW.<systemid>.BNJ36PR
SYS3.NETVIEW.<systemid>.BNJ36SE
SYS3.NETVIEW.<systemid>.DSIKPNL
SYS3.NETVIEW.<systemid>.DSILIST
SYS3.NETVIEW.<systemid>.DSILOGP
SYS3.NETVIEW.<systemid>.DSILOGS
SYS3.NETVIEW.<systemid>.DSISVRT
SYS3.NETVIEW.<systemid>.DSITRCP
SYS3.NETVIEW.<systemid>.DSITRCS
SYS3.NETVIEW.<systemid>.SDSIOPEN
```

CCI: CCI-001499

______________________________________________________________

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-50925r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETR020
Rule Title: NetView resources must be properly defined and protected.

Vulnerability Discussion: NetView can run with sensitive system privileges, and
potentially can circumvent system controls. Failure to properly control access
to product resources could result in the compromise of the operating system

environment, and compromise the confidentiality of customer data. Many
utilities
assign resource controls that can be granted to system programmers only
in
greater than read authority. Resources are also granted to certain non
systems
personnel with read only authority.

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

Check Content:
When SECOPTS.OPERSEC=SAFPW is specified in ZNET0040, this is not
applicable.

a) From the Administrator main menu, select 3;4 (Security Server Reports,
General Resource Profiles) and press ENTER.

b) Tab down to CLASS, type NETVIEW or whatever class has been set up for
Netview
Resources (find out from your IOA) on your system and press ENTER.
 1. Look for the profiles in the Profile Name column that are listed in
the
Netview Resources table, resource column in the z/OS STIG Addendum.
 2. Ensure that they are defined with a UACC=NONE in the UACC column.
 3. If all UACCs are NONE, there is NO FINDING on this point.
 4. If any UACC is not equal to NONE, this is a FINDING.

c) Type LR in the CMD column of each resource name listed in the table
below and
check that:
 1. Warning = NO.
 2. The access list showing list of users, only includes valid users per
the
resources table.
 3. The users only have the level of access permitted per the NETVIEW
Resources
table.
 ** (To check if a user belongs to one of the groups in the NETVIEW
 RESOURCES table:
 - Select Option 3;2 from the Administrator Main Menu (Security
 Server Reports, Group Profiles)
 - On the Group Reports Menu, enter 1 at the Command line (for
 Group Profile Summary)
 - Then tab down to Group and enter the
 Group Name from the resources table and hit enter.
 - On the next panel enter LV next to the group name and hit
 enter
 - The General Information Screen that comes up will have the
 list of Connected Users.
d) If
 - WARNING is not set to NO or
 - any users or groups are granted access who are not in the NETVIEW
Resource

Table or
 - any users are granted a higher level of access than is permitted to them per
the NETVIEW Resource table then 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 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.)

When SECOPTS.OPERSEC=SAFPW is specified in ZNET0040, this is not applicable. This can be bypassed.

Ensure that all NetView resources and/or generic equivalents are properly protected according to the requirements specified in the NetView Resources table in the z/OS STIG Addendum. Additional details can be obtained in the IBM Tivoli NetView for z/OS Security Reference.

Use the NetView Resources table in the z/OS STIG Addendum. This table lists the resources and access requirements for NetView, ensure the following guidelines are followed:

The RACF resource access authorizations restrict access to the appropriate personnel.

The RACF resource access authorizations specify UACC(NONE) and NOWARNING.

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

```
RDEFINE NETCMDS netid.** UACC(NONE) OWNER(ADMIN)
       AUDIT(FAILURE(READ)) DATA('Protected per ZNETR020')
RDEFINE NETCMDS netid.luname.ADDCMD.** UACC(NONE) OWNER(ADMIN)
       AUDIT(FAILURE(READ)) DATA('Protected per ZNETR020')
PERMIT netid.luname.ADDCMD.** CLASS(NETCMDS) ID(syspaudt) ACCESS(READ)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-28614r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETR030
Rule Title: NetView Started Task name(s) is not properly identified / defined to the system ACP.

Vulnerability Discussion: NetView requires a started task(s) 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:
a) Use Vanguard s Analyzer product to look at the Started Procedures Analysis report: Do the following for both CNMPSSI and CNMPROC

a. From Analyzer main Menu, go to 3;4; Press <ENTER>
b. Key in SORT PROCNAME; Press <ENTER>
c. Key in L CNMPSSI or CNMPROC; Press <ENTER>
d. If not found then CNMPSSI or CNMPROC is not defined to RACF as a STC user.
e. If found but has an R in the M column, review the message and ensure that the following does not appear: VSA346R The user ID does not have the protected attribute. If message exists, then user does not have the PROTECTED attribute. This is a finding.
f. If found then you would use the U line command to determine if the userid is defined to RACF.
g. Key the U line command for the CNMPSSI or CNMPROC entry; Press <ENTER>
h. The userid is defined to RACF if a userid display appears. If not defined you should see the message Unable to display .

b) If the userid for the CNMPSSI or CNMPROC started task is defined to the security database with the PROTECTED attribute, there is NO FINDING.

c) If the userid for the CNMPSSI or CNMPROC started task is not defined to the
security database or does not have the PROTECTED attribute, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (3)

Fix Text: The NetView system programer and the IAO will ensure that the product's Started Task(s) is properly Identified / defined to the System ACP.

Most installation manuals will indicate how the Started Task is identified and
any additional attributes that must be specified.

A sample is provided here:

```
au cnmpssi name('stc, netview') nopass dfltgrp(stc) -
owner(stc) data('netview subsystem interface')
au cnmproc name('stc, netview') nopass dfltgrp(stc) -
owner(stc) data('netview')
```

CCI: CCI-000764

---

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-28463r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETR032
Rule Title: IBM Tivoli NetView Started task(s) must be properly defined to the
STARTED resource class for RACF.

Vulnerability Discussion: Access to product resources should be restricted to
only those individuals responsible for the application connectivity and who have
a requirement to access these resources. Improper control of product resources
could potentially compromise the operating system, ACP, and customer data.

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

Check Content:
Use Vanguard s Analyzer product to look at the Started Procedures Analysis
report: The
name of the netview started task is likely CNMPROC and/or CNMPSSI. CNMPROC is

the start procedure for the NetView program and CNMPSSI starts the NetView
subsystem address space.
1. From Analyzer main Menu, go to 3;4; Press <ENTER>
2. Key in SORT PROCNAME; Press <ENTER>
3. Key in L <name of netview started task>; Press <ENTER>
4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
5. If not found then the NetView started task is not defined to RACF as a STC user.

b) If a STARTED resource class profile exists for the started task netview
(CNMPROC and/or CNMPSSI), there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for
the
started task for netview, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (2)

Fix Text: The IBM Tivoli NetView system programmer and the IAO will ensure that
a product's started task(s) is (are) properly identified and/or defined to the
System ACP.

A unique userid must be assigned for the IBM Tivoli NetView started task(s) thru
a corresponding STARTED class entry.

The following sample set of commands is shown here as a guideline:

```
rdef started CNMPROC.** uacc(none) owner(admin) audit(all(read))
stdata(user(CNMPROC) group(stc))
rdef started CNMPSSI.** uacc(none) owner(admin) audit(all(read))
stdata(user(CNMPSSI) group(stc))

setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED