

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS NetView for ACF2 STIG
Version: 6
Release: 7
29 Dec 2020

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

IACControls: 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.COMDAUTH 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 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

IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

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

- SENSITVE.RPT(NETVRPT)

Automated Analysis

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

- PDI(ZNET0000)

b) Verify that access to the NetView install data sets are properly restricted.

___ The ACF2 data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

___ The ACF2 data set rules for the datasets does not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

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

d) If any of the above is 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 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 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

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

\$KEY(SYS2)

NETVIEW.- UID(syspautd) R(A) W(L) A(L) E(A)

NETVIEW.- UID(audtaudt) R(A) E(A)

\$KEY(SYS2A)

NETVIEW.- UID(syspautd) R(A) W(L) A(L) E(A)

NETVIEW.- UID(audtaudt) R(A) E(A)

\$KEY(SYS3)

NETVIEW.- UID(syspautd) R(A) W(L) A(L) E(A)

NETVIEW.- UID(audtaudt) R(A) E(A)

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

IACControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

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

- SENSITIVE.RPT(NETVSTC)

Automated Analysis

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

- PDI(ZNET0001)

Verify that access to the NetView STC data sets are properly restricted.

___ The ACF2 data set rules for the data sets restricts READ access to auditors.

___ The ACF2 data set rules for the data sets restricts UPDATE and/or ALTER access to systems programming personnel.

___ The ACF2 data set rules for the data sets restrictS UPDATE and/or ALTER access to the product STC(s) and/or batch job(s).

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:

SET RULE

\$KEY(SYS3)

NETVIEW.<systemid>.- UID(audtautd) R(A) E(A)

NETVIEW.<systemid>.- UID(cnmproc) R(A) W(A) A(A) E(A)

NETVIEW.<systemid>.- UID(syspuot) R(A) W(A) A(A) E(A)

NETVIEW.<systemid>.- UID(tstcautd) R(A) W(A) A(A) E(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

IACControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(ZNET0020)
- ACF2CMD5.RPT(RESOURCE) Alternate report

Automated Analysis

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

- PDI(ZNET0020)

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

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

___ The ACF2 resources are defined with a default access of PREVENT.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel.

Fix Text: The IAO will 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:

```
SET RULE
$KEY(SYS3)
NETVIEW.<systemid>.- UID(audtaudt) R(A) E(A)
NETVIEW.<systemid>.- UID(cnmproc) R(A) W(A) A(A) E(A)
NETVIEW.<systemid>.- UID(sypudt) R(A) W(A) A(A) E(A)
NETVIEW.<systemid>.- UID(tstcaudt) R(A) W(A) A(A) E(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-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:

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

- ACF2CMDS.RPT(ATTSTC)

If the logonid for the NetView started task(s) includes MUSASS and NO-SMC, there is NO FINDING.

If the logonid for the NetView started task(s) is not defined or does not include MUSASS and/or NO-SMC, this is a FINDING.

Fix Text: The NetView system programmer and the ISSO will ensure that a product's 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.

Example:

SET LID
CHANGE NETVIEW STC MUSASS NO-SMC

CCI: CCI-000764

UNCLASSIFIED