VANGUARD
Integrity Professionals, Inc.

Enterprise Security Software

z/OS NetView for TSS STIG

Version: 6

Release: 8

22 Jul 2016

_____

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.

Check Content:
Review the member CxxSTYLE in the DSIPARM DD statement concatenation of the NetView CNMPROC STC procedure.

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

-      PDI(ZNET0040)

Ensure that all NetView configuration requirements are specified. If the following guidance is true, this is not a finding.

Keyword   Value
SECOPTS.OPERSEC   SAFCHECK|SAFDEF
SECOPTS.CMDAUTH   SAF.FAIL|SAF.table

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-27315r1_rule

Severity: CAT II
 Rule Version (STIG-ID): ZNETT000
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 these data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

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

___   The TSS 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. All other users can 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:

TSS PERMIT(syspaudt) DSN(SYS2.netview.) ACCESS(r)
TSS PERMIT(syspaudt) DSN(SYS2.netview.) ACCESS(all) ACTION(AUDIT)

TSS PERMIT(syspaudt) DSN(SYS2a.netview.) ACCESS(r)
TSS PERMIT(syspaudt) DSN(SYS2a.netview.) ACCESS(all) ACTION(AUDIT)

TSS PERMIT(syspaudt) DSN(SYS3.netview.) ACCESS(r)
TSS PERMIT(syspaudt) DSN(SYS3.netview.) ACCESS(all) ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002234

_____

 Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-27327r1_rule
Severity: CAT II
 Rule Version (STIG-ID): ZNETT001
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.

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

-     SENSITVE.RPT(NETVSTC)

Automated Analysis

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

-    PDI(ZNET0001)

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

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

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

___   The TSS data set rules for the data sets restricts UPDATE and/or ALL 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:

TSS PERMIT(CNMPROC) DSN(SYS3.netview.<systemid>.) ACCESS(R)
TSS PERMIT(audtaudt) DSN(SYS3.netview.<systemid>.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.netview.<systemid>.) ACCESS(R)
TSS PERMIT(tstcpaudt) DSN(SYS3.netview.<systemid>.) ACCESS(R)
TSS PERMIT(CNMPROC) DSN(SYS3.netview.<systemid>.) ACCESS(ALL)
TSS PERMIT(syspaudt) DSN(SYS3.netview.<systemid>.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.netview.<systemid>.) ACCESS(ALL)

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-50926r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETT020
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.

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

-    SENSITVE.RPT(ZNET0020)

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 TSS resources and/or generic equivalents as designated in the above table are owned or DEFPROT is specified for the resource class.

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

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 TSS resources and/or generic equivalents as designated in the above table are owned or DEFPROT is specified for the resource class.

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

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

TSS ADD(dept-acid) NETCMDS(netid)
TSS PERMIT(syspaudt) NETCMDS(netid.luname.ADDCMD) ACCESS(READ)

CCI: CCI-000035

CCI: CCI-002234
_____

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-28615r1_rule

Severity: CAT II
 Rule Version (STIG-ID): ZNETT030
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.

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

-      TSSCMDS.RPT(@ACIDS)

b)   Review the NetView STC/Batch ACID(s) for the following:

___   Is defined as CNMPROC for the ACID.

___   Is defined as CNMPSSI for the ACID.

___   Both are defined with Facility of STC and/or BATCH.

___   CNMPROC is defined with Master Facility of NETVIEW.

___   Both are sourced to the INTRDR.

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 Systems Programmer and IAO will ensure that the started task(s)
for NetView is properly defined.

Define the started task userid CNMPROC and CNMPSSI for NetView.

Example:

TSS CRE(CNMPROC) DEPT(Dept) NAME('NetView') -
 FAC(STC) MASTFAC(NETVIEW) PASSWORD(password,0) -
 SOURCE(INTRDR)
TSS CRE(CNMPSSI) DEPT(Dept) NAME('NetView') -
 FAC(STC) PASSWORD(password,0) -
 SOURCE(INTRDR)

CCI: CCI-000764

_____

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-28464r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNETT032
Rule Title: IBM Tivoli NetView Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.

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.

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

-    TSSCMDS.RPT(#STC)

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

-    PDI(ZNET0032)

Verify that the IBM Tivoli NetView started task(s) is (are) defined in the TSS STC record.

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 ACID must be assigned for the IBM Tivoli NetView started task(s) thru a corresponding STC table entry.

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

TSS ADD(STC) PROCNAME(CNMPROC) ACID(CNMPROC)
TSS ADD(STC) PROCNAME(CNMPSSI) ACID(CNMPSSI)

CCI: CCI-000764

_____

Group ID (Vulid): V-17469

Group Title: ZB000036
Rule ID: SV-28465r1_rule
Severity: CAT II
 Rule Version (STIG-ID): ZNETT036
Rule Title: NetView is not properly defined to the Facility Matrix Table for Top Secret.

Vulnerability Discussion: Improperly defined security controls for the Product could result in the compromise of the network, operating system, and customer data.

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

-      TSSCMDS.RPT(FACLIST) - Preferred report containing all control option values in effect including default values
-      TSSCMDS.RPT(TSSPRMFL) - Alternate report containing only control option values explicitly coded at TSS startup

b)   If NETVIEW is properly defined in the Facility Matrix table, there is NO FINDING:

c)   If NETVIEW is improperly defined in the Facility Matrix table, this is a FINDING.

Fix Text: Define NETVIEW as a Facility to TOP SECRET in the Facility Matrix Table using the following example:

**** NETVIEW
*
FACILITY(USERxx=NAME=NETVIEW)
FACILITY(NETVIEW=MODE=FAIL)
FACILITY(NETVIEW=PGM=DSI)
FACILITY(NETVIEW=ACTIVE,SHRPRF,ASUBM,ABEND,MULTIUSER,NOXDEF)
FACILITY(NETVIEW=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT)

FACILITY(NETVIEW=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFTRANS,IJU)

FACILITY(NETVIEW=MSGLC,NOTRACE,NOEODINIT,NODORMPW,NONPWR)

FACILITY(NETVIEW=LOG(INIT,SMF,MSG,SEC9))

FACILITY(NETVIEW=DOWN=GLOBAL,LOCKTIME=00,DEFACID(*NONE*))

CCI: CCI-000764
_____