

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS Quest NC-Pass for TSS STIG

Version: 6

Release: 2

20 Jan 2015

Group ID (Vulid): V-16932

Group Title: ZB000000

Rule ID: SV-40865r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZNCPT000

Rule Title: Quest NC-Pass installation data sets will be properly protected.

Vulnerability Discussion: Quest NC-Pass installation data sets have the ability 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.

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

Check Content:

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

- SENSITIVE.RPT(NCPASRPT)

Automated Analysis

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

- PDI(ZNCP0000)

Verify that the accesses to the Quest NC-Pass installation data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS data set rules for the data sets restricts READ access to all authorized users.

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

___ The TSS data set rules for the data sets specify that all (i.e., failures and successes) WRITE and/or greater access is logged.

Fix Text: The IAO will ensure that WRITE and/or greater access to Quest NC-Pass installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to all authorized users.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have WRITE and/or greater access

and if required that all WRITE and/or greater access is logged. He will identify if any additional groups have WRITE and/or greater 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.NCPASS.

SYS3.NCPASS. (data sets that are not altered by product STCs, can be more specific)

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

```
TSS PERMIT(<sypaudt>) DSN(SYS2.NCPASS.) ACCESS(R)
TSS PERMIT(<sypaudt>) DSN(SYS2.NCPASS.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS2.NCPASS.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS2.NCPASS.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.NCPASS.) ACCESS(R)
TSS PERMIT(ALL) DSN(SYS2.NCPASS.) ACCESS(R)
TSS PERMIT(<sypaudt>) DSN(SYS3.NCPASS.) ACCESS(R)
TSS PERMIT(<sypaudt>) DSN(SYS3.NCPASS.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.NCPASS.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS3.NCPASS.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS3.NCPASS.) ACCESS(R)
TSS PERMIT(*) DSN(SYS3.NCPASS.) ACCESS(R)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067

Group Title: ZB000001

Rule ID: SV-40868r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZNCPT001

Rule Title: Quest NC-Pass STC data sets will be properly protected.

Vulnerability Discussion: Quest NC-Pass STC data sets have the ability 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.

IAControls: 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(NCPASSTC)

Automated Analysis

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

- PDI(ZNCP0001)

Verify that the accesses to the Quest NC-Pass 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 access to domain level security administrators.

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

___ The TSS data set rules for the data sets restricts WRITE and/or greater access to the Quest NC-Pass's STC(s) and/or batch user(s).

Fix Text: The IAO will ensure that WRITE and/or greater access to Quest NC-Pass STC data sets is limited to System Programmers and/or Quest NC-Pass's STC(s) and/or batch user(s) only. UPDATE access can be given to domain level security administrators. READ access can be given to auditors.

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.NCPASS.*.PASSCAF

SYS3.NCPASS.*.PASSVSD

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

TSS PERMIT(<syspautd>) DSN(SYS3.NCPASS.*.PASSCAF) ACCESS(ALL)

TSS PERMIT(<tstcaudt>) DSN(SYS3.NCPASS.*.PASSCAF) ACCESS(ALL)

TSS PERMIT(NCASS STCs) DSN(SYS3.NCPASS.*.PASSCAF) ACCESS(ALL)
TSS PERMIT(<secaudt>) DSN(SYS3.NCPASS.*.PASSCAF) ACCESS(U)
TSS PERMIT(<audtaudt>) DSN(SYS3.NCPASS.*.PASSCAF) ACCESS(R)
TSS PERMIT(<sypaudt>) DSN(SYS3.NCPASS.*.PASSVSDD) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.NCPASS.*.PASSVSDD) ACCESS(ALL)
TSS PERMIT(NCASS STCs) DSN(SYS3.NCPASS.*.PASSVSDD) ACCESS(ALL)
TSS PERMIT(<secaudt>) DSN(SYS3.NCPASS.*.PASSVSDD) ACCESS(U)
TSS PERMIT(<audtaudt>) DSN(SYS3.NCPASS.*.PASSVSDD) ACCESS(R)

CCI: CCI-001499

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-40871r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZNCPT020

Rule Title: Quest NC-Pass will be used by Highly-Sensitive users.

Vulnerability Discussion: DISA has directed that Quest NC-Pass extended authentication be implemented on all domains. All users with update and alter access to sensitive system-level data sets and resources, or who possess special security privileges, are required to use NC-Pass for extended authentication. Typical personnel required to use NC-Pass include, but are not limited to, systems programming, security, operations, network/communications, storage management, and production control.

Improper enforcement of extended authentication through NC-Pass could potentially compromise the operating system, ACP, and customer data.

IAControls: ECCD-1, ECCD-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)
- TSSCMDS.RPT(@ALL)
- SENSITIVE.RPT(WHOHABS)

If all sensitive users requiring NC-Pass validation has the NCPASS Facility and permitted to the SECURID resource in the ABSTRACT resource class, this is not a finding.

NOTE: Sensitive users include systems programming personnel, security personnel, and other staff (e.g., DASD management, operations, auditors, technical support, etc.) with access to sensitive resources (e.g., operator

commands, ACP privileges, etc.) that can modify the operating system and system software, and review/modify the security environment.

Fix Text: The IAO will ensure that sensitive users are properly validated to Quest NC-Pass.

NOTE: Sensitive users include systems programming personnel, security personnel, and other staff (e.g., DASD management, operations, auditors, technical support, etc.) with access to sensitive resources (e.g., operator commands, ACP privileges, etc.) that can modify the operating system and system software, and review/modify the security environment.

Sensitive users requiring access to NC-PASS must be granted access to the NCPASS Facility and the SECURID resource in the ABSTRACT resource class. Use the following commands as an example:

```
TSS ADD(acid) FAC(NCPASS)
TSS PERMIT(acid) ABS(SECURID)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-40874r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZNCPT030

Rule Title: Quest NC-Pass Started Task name will be properly identified and/or defined to the system ACP.

Vulnerability Discussion: Quest NC-Pass 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.

IAControls: ECCD-1, ECCD-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)

Verify that the ACID(s) for the Quest NC-Pass started task(s) is (are) properly defined. If the following attributes are defined, this is not a finding.

FACILITY(STC, BATCH)
PASSWORD(xxxxxxxx,0)
SOURCE(INTRDR)
NOSUSPEND
MASTFAC(NCPASS)

Fix Text: The IAO working with the systems programmer will ensure the Quest NC-Pass Started Task(s) is properly identified and/or 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.

The following commands are provided as a sample for defining Started Task(s):

```
TSS CREATE(NCPASS) TYPE(USER) -  
    NAME('STC, Quest NC-Pass') DEPT(xxxx) -  
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -  
    SOURCE(INTRDR) NOSUSPEND  
    MASTFAC(NCPASS)
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-40876r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNCPT032
Rule Title: Quest NC-Pass Started task will 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.

IAControls: ECCD-1, ECCD-2

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(ZNCP0032)

If the Quest NC-Pass started task(s) is (are) defined in the TSS STC record, this is not a finding.

Fix Text: The IAO working with the systems programmer will ensure the Quest NC-Pass Started Task(s) is properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the CA 1 Tape Management started task(s) thru a corresponding STC table entry.

The following commands are provided as a sample for defining Started Task(s):

TSS ADD(STC) PROCNAME(NCPASS) ACID(NCPASS)

CCI: CCI-000764

Group ID (Vulid): V-17469

Group Title: ZB000036

Rule ID: SV-40877r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZNCPT036

Rule Title: Quest NC-Pass will be properly defined to the Facility Matrix Table.

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

IAControls: ECCD-1, ECCD-2

Check Content:

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

- TSSCMDS.RPT(FACLST) - 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

If the Quest NC-Pass Facility Matrix table is defined as stated below, this is not a finding.

FACILITY DISPLAY FOR NCPASS
INITPGM=NCS ID=14 TYPE=099
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
ATTRIBUTES=LUUPD
MODE=FAIL DOWN=GLOBAL LOGGING=INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
MAXUSER=03000 PRFT=003

Fix Text: The IAO working with the systems programmer will ensure the Facility Matrix Table for Quest NC-Pass is proper defined using the following example:

*****NCPASS
FAC(USERxx=NAME=NCPASS,PGM=NCS,ID=nn,ACTIVE,NOASUBM)
FAC(NCPASS=LUMSG,STMSG,NORNDPW,WARNPW,MODE=FAIL)
FAC(NCPASS=LOG(SMF,INIT,MSG,SEC9),UIDACID=8,LOCKTIME=000)

CCI: CCI-000764

UNCLASSIFIED