

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS Quest NC-Pass for RACF STIG

Version: 6

Release: 3

30 June 2023

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

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-40864r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNCPR000
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.

Responsibility: Information Assurance Officer
IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the names of the QUEST NC-PASS product datasets. (They may begin with SYS2.CCS, SYS2A.CS., or SYS3.CCS).

b) Ensure the following data set controls are in effect for the QUEST NC-PASS product data sets:

- UPDATE or higher access to the QUEST NC-PASS product data sets is restricted to systems programming personnel.
- UACC (None) and NOWARNING are specified for the QUEST NC-PASS product data sets..
- The RACF data set rules for the QUEST NC-PASS data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.
2. Tab down to Data Set row, type LV next to the dataset profile for the QUEST NC-PASS data sets.
3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
4. Review the Universal Access and Access List on the dataset profile General Information Screen..
5. Repeat steps 1-3 above for any other QUEST NC-PASS dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the QUEST NC-PASS product data sets are restricted to systems programming personnel, there is NO FINDING.

e) If UPDATE and ALLOCATE (ALTER) access to the CA -1 product data sets is not restricted to systems programming personnel, this is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING

g) .IF UACC is not None or Warning is not No, this is a FINDING..

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:

```
ad 'SYS2.NCPASS.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('Quest NC-Pass Install DS')
pe 'SYS2.NCPASS.**' id(<syspau< <tstcaudt>) acc(a)
pe 'SYS2.NCPASS.**' id(<audtaudt>) acc(r)
pe 'SYS2.NCPASS.**' id(*) acc(r)
```

```
ad 'SYS3.NCPASS.**' uacc(none) owner(sys3) -
    audit(success(update) failures(read)) -
    data('Quest NC-Pass Install DS')
pe 'SYS3.NCPASS.**' id(<syspau< <tstcaudt>) acc(a)
pe 'SYS3.NCPASS.**' id(<audtaudt>) acc(r)
pe 'SYS3.NCPASS.**' id(*) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-40867r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNCPR001
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.

Responsibility: Information Assurance Officer
IAControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Create a dataset (DSORG: FB LRECL: 80) with a list of the NC-PASS data sets referenced in Section 6.3.2, NC-PASS for RACF, in the Z/OS STIG. Enter each dataset on its own line and starting in column 1.

Note: Use ISPF 3.4 with the high-level qualifiers for the NC-PASS datasets to assist in generating the list of datasets.

- b) From Analyzer main Menu, go to 3;B; Press ENTER
- c) Place an S next to User defined list. Key in the name of the dataset created in step (a) in the Fully qualified (without quotes) name of data set containing list: field. Press ENTER
- d) Place an R next one of the entries in the report. Press ENTER
1. If the RACF data set rules restrict UPDATE and/or ALTER access to Z/OS systems programming personnel and/or security personnel, there is NO FINDING.
 2. If the RACF data set rules restrict UPDATE access to the NC-PASS started task user ID, there is NO FINDING.
- e) If (d1) or (d2) is untrue, there is a FINDING.

- f) Repeat steps (d) (d1) and (d2) for each dataset in the list.

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.*.PASSVSDD

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

```
ad 'SYS3.NCPASS.*.PASSCAF.**' uacc(none) owner(sys3) -
    audit(failures(read)) -
    data('Vendor DS Profile: Quest NC-Pass')
ad 'SYS3.NCPASS.*.PASSVSDD.**' uacc(none) owner(sys3) -
    audit(failures(read)) -
    data('Vendor DS Profile: Quest NC-Pass')
pe ' SYS3.NCPASS.*.PASSCAF.**' id(<syspautd> <tstcaudt> NCPASS STCs)
acc(a)
pe ' SYS3.NCPASS.*.PASSCAF.**' id(<secaudt>) acc(u)
pe ' SYS3.NCPASS.*.PASSCAF.**' id(<audtaudt>) acc(r)
pe ' SYS3.NCPASS.*.PASSVSDD.**' id(<syspautd> <tstcaudt> NCPASS STCs)
acc(a)
pe ' SYS3.NCPASS.*.PASSVSDD.**' id(<secaudt>) acc(u)
pe ' SYS3.NCPASS.*.PASSVSDD.**' id(<audtaudt>) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-001499

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-40870r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZNCPR020
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.

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

Check Content:

- a) From Administrator main Menu, go to 3;15; Press ENTER
- b) Key in SECURID in the Group field. Press ENTER.
- c) If their report contains only the line NO CONNECTS TO REPORT, then SECURID is not defined as a group and there is a FINDING.
- d) If there is a SECURID group, then key in CS next the SECURID entry and press Enter
- e) Examine the list of user IDs in the Connect Summary report and ensure that Sensitive users (see note below) that require NC-PASS validation are connected to the SECURID group. If not, there is 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.

Ensure SECURID is defined to RACF. Use the following RACF AddGroup command:

```
AG SECURID SUPGROUP(ADMIN) OWNER(ADMIN)
```

Ensure sensitive users that require NC-Pass validation is connected to the SECURID group. Use the following command:

```
CO userid GROUP(SECURID) OWNER(SECURID)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
 Group Title: ZB000030
 Rule ID: SV-40873r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZNCPR030
 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.

Responsibility: Information Assurance Officer

IAControls: ECCD-1, ECCD-2

Check Content:

- a) From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press ENTER
- b) Look for STARTED in the Source column, NCPASS in the Procname column and * in the Jobname column.
- c) If the NC-PASS started task does not have an R in the M column there is NO FINDING. An R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)
- d) If there is an R in the M column, there is 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.

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):

```
au NCPASS name('STC, Quest NC-Pass') owner(stc) dfltgrp(stc) nopass
    data('Start CA1 TMS')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
 Group Title: ZB000032
 Rule ID: SV-40875r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZNCPR032
 Rule Title: Quest NC-Pass Started task will 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
 IACControls: ECCD-1, ECCD-2

Check Content:

- a) From Analyzer main Menu, go to 3;4; Press ENTER
- b) Look for STARTED in the Source column, NCPASS in the Procname column and * in the Jobname column. If the entry exists, there is NO FINDING.
- c) If the entry looked for in step (b) above is not found, this is 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):

```
rdef started NCPASS.** uacc(none) owner(admin) audit(all(read))
      stdata(user(NCPASS) group(stc))
setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED