

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS Quest NC-Pass for ACF2 STIG
Version: 6
Release: 2
29 Dec 2020

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
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 ACF2 data set rules for the data sets restricts READ access to all authorized users.

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

___ The ACF2 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:

\$KEY(SYS2)

NCPASS.- UID(<syspau>) R(A) W(L) A(L) E(A)

NCPASS.- UID(<stcaudt>) R(A) W(L) A(L) E(A)

NCPASS.- UID(<audtaudt>) R(A) E(A)

NCPASS.- UID(*) R(A) E(A)

\$KEY(SYS3)

NCPASS.- UID(<syspau>) R(A) W(L) A(L) E(A)

NCPASS.- UID(<stcaudt>) R(A) W(L) A(L) E(A)

NCPASS.- UID(<audtaudt>) R(A) E(A)

NCPASS.- UID(*) R(A) E(A)

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

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

___ The ACF2 data set rules for the data sets restricts WRITE access to domain level security administrators.

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

___ The ACF2 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:

\$KEY(SYS3)

NCPASS-.PASSCAF.- UID(<syspau>) R(A) W(A) A(A) E(A)
NCPASS-.PASSCAF.- UID(<tstcaudt>) R(A) W(A) A(A) E(A)
NCPASS-.PASSCAF.- UID(NCPASS STCs) R(A) W(A) A(A) E(A)
NCPASS-.PASSCAF.- UID(secaudt) R(A) W(A) E(A)
NCPASS-.PASSCAF.- UID(<audtaudt>) R(A) E(A)
NCPASS-.PASSVSDD.- UID(<syspau>) R(A) W(A) A(A) E(A)
NCPASS-.PASSVSDD.- UID(<tstcaudt>) R(A) W(A) A(A) E(A)
NCPASS-.PASSVSDD.- UID(NCPASS STCs) R(A) W(A) E(A)
NCPASS-.PASSVSDD.- UID(<secaudt>) R(A) W(A) E(A)
NCPASS-.PASSVSDD.- UID(<audtaudt>) R(A) E(A)

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
IAControls: ECCD-1, ECCD-2

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

- ACF2CMD5.RPT(TSOUSERS)

If all sensitive users requiring NC-Pass validation has the AUTHSUP1 attribute, 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.

The following attributes must be set for logonids requiring NC-Pass validation:

SET LID
CHANGE logonid AUTHSUP1

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

- ACF2CMDS.RPT(ATTSTC)

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

finding.

STC
MUSASS
NO-SMC
MUSUPDT

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

UNCLASSIFIED