

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS CA VTape for RACF STIG

Version: 6

Release: 5

30 June 2023

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

Group ID (Vulid): V-224444
Group Title: ZB000000
Rule ID: SV-33825r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZVTAR000
Rule Title: CA VTape installation data sets are not properly protected.

Vulnerability Discussion: CA VTape 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(VTARPT)

Automated Analysis

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

- PDI(ZVTA0000)

Verify that the accesses to the CA VTape installation data sets are properly restricted.

____ The RACF data set rules for the data sets restricts READ access to all authorized users.

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

____ The RACF data set rules for the data sets specify that all (i.e., failures and successes) UPDATE and/or ALTER access are logged.

Fix Text:

The IAO will ensure that update and alter access to CA VTape installation data sets is limited to System Programmers only, and all update and alter 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 update and alter access and if required that all update and alter 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:
SYS2.VTAPE.**

SYS3.VTAPE.** (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.VTAPE.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('CA VTAPE Install DS')
pe 'SYS2.VTAPE.**' id(<syspau> <tstcaudt>) acc(a)
pe 'SYS2.VTAPE.**' id(<audtaudt> authorized users) acc(r)
pe 'SYS2.VTAPE.**' id(VTAPE STCs)
```

```
ad 'SYS3.VTAPE.**' uacc(none) owner(sys3) -
    audit(success(update) failures(read)) -
    data('CA VTAPE Install DS')
pe 'SYS3.VTAPE.**' id(<syspau> <tstcaudt>) acc(a)
pe 'SYS3.VTAPE.**' id(<audtaudt> authorized users) acc(r)
pe 'SYS3.VTAPE.**' id(VTAPE STCs)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid): V-224445
 Group Title: ZB000001
 Rule ID: SV-33828r2_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZVTAR001
 Rule Title: CA VTAPE STC data sets will be properly protected.

Vulnerability Discussion: CA VTAPE 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:

a) Check with your IOA or Systems Programming personnel and compile the list of

CA VTape product installation data sets. Likely these data set names will

start with SYS3.VTAPE.

b). Do the following:

1. From the Administrator Main Menu Choose Option 2 - Security Server Commands

2. Then choose Option 3 - Data Set

3. Tab to Enter fully qualified (without quotes) data set or profile name:

and enter the name of the first CA VTape product installation data set found in

a.

above..

4. Hit Enter.

5. For the resulting pop-up, select Y when prompted with Display covering profile?.

6. On the next screen ,

a. Verify that the UACC is NONE

b. Verify that all accesses of UPDATE or higher (i.e., failures and successes)

will be

logged. Look at the section of the screen under Audit:. Next to Successes and

Failures you should see Update.

c. Tab down to ;Standard Access Permits and type an E and hit Enter.

d. On the next screen verify that UPDATE, and/or ALTER access is permitted

to systems programming personnel, tape management personnel (tape librarians

and any other users that perform control, initialization, and maintenance of

the

systems tape library) and CA VTape STCs and/or CA VTape batch userids..

e. Check if the Conditional Access Permits: section on the screen has the

phrase *data is present* next to it.

If so, enter an E on the line and hit Enter to get a list of

who has Conditional Access Permits.

f. Verify that Conditional Access Permits of UPDATE, and/or ALTER access are

restricted to systems programming personnel, tape management personnel (tape

librarians and any other users that perform control initialization and maintenance of the systems tape library) and CA VTape STCs and/or CA VTape batch userids.

7. Repeat steps 3 through 6 for all the CA VTape datasets found in a. above.

c) If 6a, 6b, 6d and 6f above are all true, there is NO FINDING.

d) If 6a, 6b, 6d and 6f above are NOT all true, there is a FINDING.

Fix Text: The IAO will ensure that WRITE and/or greater access to CA VTape STC data sets is limited to System Programmers, Tape Management personnel and/or CA VTape s STC(s) and/or batch user(s) only. READ access can be given to auditors and authorized users.

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.VTAPE (data sets that are altered by the product s STCs, this can be more specific)

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

```
ad 'SYS3.VTAPE.**' uacc(none) owner(sys3) -
    audit(failures(read)) -
    data('Vendor DS Profile: CA VTAPE')
pe 'SYS3.VTAPE.**' id(<syspau> <tstcaudt> VTAPE STCs) acc(a)
pe 'SYS3.VTAPE.**' id(<tapeaudt> VTAPE STCs) acc(a)
pe 'SYS3.VTAPE.**' id(<audtaudt> authorized users) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-001499

Group ID (Vulid): V-224446
 Group Title: ZB000030
 Rule ID: SV-33831r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZVTAR030
 Rule Title: CA VTape Started Task name is not properly identified/defined to the system ACP.

Vulnerability Discussion: CA VTape 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
 IACControls: ECCD-1, ECCD-2

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

- RACFCMDS.RPT(LISTUSER)

The CA VTape started task(s) and/or batch job userid(s) is defined and is assigned the RACF PROTECTED attribute.

Fix Text: The CA VTape system programmer and the IAO 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.

A sample is provided here:

```
au SVTS name('CA VTape') owner(stc) dfltgrp(stc) nopass
au SVTSAS name('CA VTape') owner(stc) dfltgrp(stc) nopass
```

CCI: CCI-000764

Group ID (Vulid): V-224447
 Group Title: ZB000032
 Rule ID: SV-33833r2_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZVTAR032
 Rule Title: CA VTape Started task(s) must 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
IAControls: ECCD-1, ECCD-2

Check Content:

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

- DSMON.RPT(RACSPT)

Automated Analysis

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

- PDI(ZVTA0032)

Verify that the CA VTape started task(s) is (are) defined to the STARTED resource class profile and/or ICHRIN03 table entry.

Fix Text: The CA VTape 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 userid must be assigned for the CA VTape started task(s) thru a corresponding STARTED class entry.

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

```
rdef started SVTS.** uacc(none) owner(admin) audit(all(read))
stdata(user(SVTS)
group(stc))
rdef started SVTSAS.** uacc(none) owner(admin) audit(all(read))
stdata(user(SVTSAS) group(stc))

setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED