

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS CA VTape for ACF2 STIG

Version: 6

Release: 4

29 Dec 2020

Group ID (Vulid): V-16932

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

IACControls: 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 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 UPDATE and/or ALTER access to systems programming personnel.

___ The ACF2 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 allocate access to CA VTape installation data sets is limited to System Programmers only, and all update and allocate 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 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:

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:

\$KEY(SYS2)

VTape.- UID(<syspautd>) R(A) W(L) A(L) E(A)

VTape.- UID(<tstcaudt>) R(A) W(L) A(L) E(A)

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

VTape.- UID(authorized users) R(A) E(A)

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

VTape.- UID(VTAPE STCs) R(A) E(A)

\$KEY(SYS3)

VTape.- UID(<syspautd>) R(A) W(L) A(L) E(A)

VTape.- UID(<tstcaudt>) R(A) W(L) A(L) E(A)

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

VTape.- UID(authorized users) R(A) E(A)

VTape.- UID(VTAPE STCs) R(A) E(A)

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid): V-17067

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:

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

- SENSITVE.RPT(VTASTC)

Automated Analysis

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

- PDI(ZVTA0001)

Verify that the accesses to the CA VTape STC 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 auditors and authorized users.

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

___ The ACF2 data set rules for the data sets restricts WRITE and/or greater access to the CA VTape s STC(s) and/or batch user(s).

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.

Example:

```
SET LID
INSERT SVTS STC NO-SMC
INSERT SVTSAS STC NO-SMC
```

CCI: CCI-001499

Group ID (Vulid): V-17452

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 ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

Insure that the logonids(s) for the CA VTape started task(s) includes the following:

STC

NO-SMC

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

UNCLASSIFIED

