VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS CA VTAPE for TSS STIG

Version: 6

Release: 4

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-33826r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZVTAT000
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.

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:

- SENSITVE.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 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 UPDATE and/or ALL access to systems programming personnel.

___ The TSS data set rules for the data sets specify that all (i.e., failures and successes) UPDATE and/or ALL 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:

TSS PERMIT(<syspaudt>) DSN(SYS2.VTAPE.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2.VTAPE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS2.VTAPE.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS2.VTAPE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.VTAPE.) ACCESS(R)
TSS PERMIT(authorized users) DSN(SYS2.VTAPE.) ACCESS(R)
TSS PERMIT(VTAPE STCs) DSN(SYS2.VTAPE.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS3.VTAPE.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS3.VTAPE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.VTAPE.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS3.VTAPE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS3.VTAPE.) ACCESS(R)
TSS PERMIT(authorized users) DSN(SYS3.VTAPE.) ACCESS(R)
TSS PERMIT(VTAPE STCs) DSN(SYS3.VTAPE.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-33829r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZVTAT001
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.

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:

- 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 TSS data set rules for the data sets restricts READ access to auditors and authorized users.

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

___ The TSS 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 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:

TSS PERMIT(<syspaudt>) DSN(SYS3.VTAPE) ACCESS(ALL)
TSS PERMIT(<tapeaudt>) DSN(SYS3.VTAPE) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.VTAPE) ACCESS(ALL)
TSS PERMIT(VTAPE STCs) DSN(SYS3.VTAPE) ACCESS(ALL)

TSS PERMIT(<audtaudt>) DSN(SYS3.VTAPE) ACCESS(R)
TSS PERMIT(authorize user) DSN(SYS3.VTAPE) ACCESS(R)

CCI: CCI-001499

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-33832r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZVTAT030
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.

IAControls: ECCD-1, ECCD-2

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

- TSSCMDS.RPT(@ACIDS)

Review each CA VTAPE STC/Batch ACID(s) for the following:

___ Defined with Facility of STC and/or BATCH for SVTS and SVTAS.

___ Is sourced to the INTRDR.

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:

```
TSS CREATE(SVTS) TYPE(USER) -
     NAME('CA VTAPE') DEPT(xxxx) -
```

```
    FAC(STC) -
    PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
TSS CREATE(SVTSAS) TYPE(USER) -
     NAME('CA VTAPE') DEPT(xxxx) -
    FAC(STC) -
    PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-33834r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZVTAT032
Rule Title: CA VTAPE Started task(s) must 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(ZVTA0032)

Verify that the CA VTAPE started task(s) is (are) defined in the TSS STC record.

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 ACID must be assigned for the CA VTAPE started task(s) thru a corresponding STC table entry.

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

TSS ADD(STC) PROCNAME(CVTS) ACID(CVTS)
TSS ADD(STC) PROCNAME(CVTSAS) ACID(CVTSAS)

CCI: CCI-000764
