VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS TADz for TSS STIG

Version: 6

Release: 6

22 Apr 2016

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-28471r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZTADT000
Rule Title: Tivoli Asset Discovery for z/OS (TADz) Install data sets are not properly protected.

Vulnerability Discussion: Tivoli Asset Discovery for z/OS (TADz) Install data sets provide the capability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Check Content:
a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(TADZRPT)

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

- PDI(ZTAD0000)

b) Verify that access to the TADz Install data sets are properly restricted.

___ The TSS data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

___ The TSS data set rules for the data sets does not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

c) If all of the above are untrue, there is NO FINDING.

d) If any of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that update and allocate/create access to program product data sets is limited to System Programmers only, and all update and allocate/create access is logged. Auditors should have read access.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have update and allocate/create

access and if required that all update and allocate/create access is logged. He will identify if any additional groups have update 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.TADZ
SYS2.TADZ .V-.SHSIMOD1 (optional fully-qualified APF).
SYS3.TADZ

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

TSS PERMIT(syspaudt) DSN(SYS2.TADZ.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS2.TADZ.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(audtaudt) DSN(SYS2.TADZ.) ACCESS(R)

TSS PERMIT(syspaudt) DSN(sys2.tadz.*.shsimod1) ACCESS(R)
TSS PERMIT(syspaudt) DSN(sys2.tadz.*.shsimod1) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(audtaudt) DSN(SYS2.TADZ.*.shsimod1) ACCESS(R)

TSS PERMIT(syspaudt) DSN(SYS3.TADZ.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.TADZ.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(audtaudt) DSN(SYS3.TADZ.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-28549r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZTADT001
Rule Title: Tivoli Asset Discovery for zOS (TADz) STC and/or batch data sets are not properly protected.

Vulnerability Discussion: Tivoli Asset Discovery for zOS (TADz) STC and/or batch data sets provide the capability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

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

- SENSITVE.RPT(TADZSTC)

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

- PDI(ZTAD0001)

For all (TADz) STC and/or batch data sets:

If the UPDATE or greater access is restricted to systems programming personnel and the product STC(s) and/or batch job(s) this is not a finding.

If any job scheduling products are in use and access is restricted to READ this is not a finding.

If auditors have READ access this is not a finding.

Fix Text: Grant update and alter access to Tivoli Asset Discovery for z/OS (TADz) STC and/or batch data sets are limited to system programmers and TADz STC and/or batch jobs only.

Grant Read access to any scheduling products that are in use.

Grant Read access to auditors at the ISSO's discretion.

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. Identify if any additional groups have update access for specific data sets, and assure that they are properly restricted to the ACP (Access Control Program) active on the system.

Data sets to be protected will be:
SYS3.TADZ

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

TSS PERMIT(syspaudt) DSN(sys3.tadz.*.iq*.) ACCESS(R)
TSS PERMIT(tadzmon) DSN(sys3.tadz.*.iq*.) ACCESS(R)
TSS PERMIT(tadzinq) DSN(sys3.tadz.*.iq*.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(sys3.tadz.*.iq*.) ACCESS(ALL)
TSS PERMIT(tadzmon) DSN(sys3.tadz.*.iq*.) ACCESS(ALL)

TSS PERMIT(tadzinq) DSN(sys3.tadz.*.iq*.) ACCESS(ALL)
TSS PERMIT(syspaudt) DSN(sys3.tadz.*.uiq.) ACCESS(R)
TSS PERMIT(tadzmon) DSN(sys3.tadz.*.uiq.) ACCESS(R)
TSS PERMIT(tadzinq) DSN(sys3.tadz.*.uiq.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(sys3.tadz.*.uiq.) ACCESS(ALL)
TSS PERMIT(tadzmon) DSN(sys3.tadz.*.uiq.) ACCESS(ALL)
TSS PERMIT(tadzinq) DSN(sys3.tadz.*.uiq.) ACCESS(ALL)
TSS PERMIT(syspaudt) DSN(sys3.tadz.*.um.) ACCESS(R)
TSS PERMIT(tadzmon) DSN(sys3.tadz.*.um.) ACCESS(R)
TSS PERMIT(tadzinq) DSN(sys3.tadz.*.um.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(sys3.tadz.*.um.) ACCESS(ALL)
TSS PERMIT(tadzmon) DSN(sys3.tadz.*.um.) ACCESS(ALL)
TSS PERMIT(tadzinq) DSN(sys3.tadz.*.um.) ACCESS(ALL)

CCI: CCI-001499

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-28555r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZTADT030
Rule Title: Tivoli Asset Discovery for z/OS (TADz) Started Task name(s) must be properly identified / defined to the system ACP.

Vulnerability Discussion: Tivoli Asset Discovery for z/OS (TADz) requires a started task(s) that will be restricted to certain resources, datasets and other system functions. By defining the started task as a userid to the system Access Control Program (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.

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

- TSSCMDS.RPT(@ACIDS)

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

___ Is defined with Facility of STC and/or BATCH.

___ Is sourced to the INTRDR.

If all of the above are true, there is NO FINDING.

If any of the above is untrue, this is a FINDING.

Fix Text: The TADz Systems Programmer and ISSO will ensure that the started task(s) for TADz is properly defined.

Define the started task for TADz.

Example:

TSS CRE(TADZMON) DEPT(Dept) NAME('TADz STC') -
FAC(STC) PASSWORD(password,0) -
SOURCE(INTRDR)

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-28562r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZTADT032
Rule Title: IBM Tivoli Asset Discovery for zOS (TADz) 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.

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(ZTAD0032)

Verify that the IBM Tivoli Asset Discovery for zOS (TADz) started task(s) is (are) defined in the TSS STC record.

Fix Text: The IBM Tivoli Asset Discovery for zOS (TADz) 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 IBM Tivoli Asset Discovery for zOS (TADz) 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(TADZMON) ACID(TADZMON)

CCI: CCI-000764
