

# **VANGUARD**

**Integrity Professionals, Inc.**

---

**Enterprise Security Software**

z/OS TADz for ACF2 STIG

Version: 6

Release: 6

29 Dec 2020

---

Group ID (Vulid): V-16932

Group Title: ZB000000

Rule ID: SV-28470r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZTADR000

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.

Responsibility: Information Assurance Officer

IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

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

- SENSITIVE.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 ACF2 data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

\_\_\_\_ The ACF2 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 access to program product data sets is limited to System Programmers only, and all update and allocate 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 alter access and if required that all update and allocate 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

SYS3.TADZ

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

\$KEY(SYS2)

TADZ.- UID(syspauDt) R(A) W(L) A(L) E(A)

TADZ.V-.SHSIMOD1 UID(syspauDt) R(A) W(L) A(L) E(A)

TADZ.- UID(audtaudt) R(A) E(A)

\$KEY(SYS3)

TADZ.- UID(syspauDt) R(A) W(L) A(L) E(A)

TADZ.- UID(audtaudt) R(A) E(A)

CCI: CCI-000213

CCI: CCI-002234

---

Group ID (Vulid): V-17067

Group Title: ZB000001

Rule ID: SV-28548r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZTADR001

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.

Responsibility: Information Assurance Officer

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:

- SENSITIVE.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:

\$KEY(SYS3)

TADZ.- UID(syspauDt) R(A) W(A) A(A) E(A)  
TADZ.- UID(audtaudt) R(A) E(A)  
TADZ.-.UM.- UID(batchid TADZINQ) R(A) W(A) A(A) E(A)  
TADZ.-.IQ.- UID(batchid TADZINQ) R(A) W(A) A(A) E(A)  
TADZ.-.UIQ.- UID(batchid TADZINQ) R(A) W(A) A(A) E(A)  
TADZ.- UID(stc id TADZMON) R(A) W(A) A(A) E(A)

CCI: CCI-001499

---

Group ID (Vulid): V-17452  
Group Title: ZB000030  
Rule ID: SV-28554r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZTADR030  
Rule Title: Tivoli Asset Discovery for z/OS (TADz) Started Task name(s) is not properly identified / defined to the system ACP.

Vulnerability Discussion: Products that require a started task will require that the started task 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(LOGONIDS)

Ensure the following field is completed for each STC logonid for the product:

STC

Ensure the following field is completed for each Batch logonid for the product:

JOB

If the logonids specified in (b) and/or (c) have all the required field is completed, this is not a FINDING.

If the logonids specified in (b) and/or (c) do not have the above field completed, this is a FINDING.

Fix Text: The TADz system programmer and the ISSO 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  
CHANGE TADZMON STC

CCI: CCI-000764

---

UNCLASSIFIED