

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS TADz for RACF STIG

Version: 6

Release: 7

30 June 2023

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

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

Tivoli Asset Discovery for z/OS Installation Datasets, Likely:

1. hlq.TADZ.

hlq.TADZ.*.SHSIMOD1.**

2. From the Administrator Main Menu choose Option 2 Security Server Commands

3. then choose Option: 3 Data Set

4. Type the resource names collected in option a.1 above into: Enter fully

qualified (without quotes) data set or profile name:

5. Hit enter.

6. Enter Y for Display covering profile? Y

7. Verify that the UACC is NONE

8. Verify that Audit Successes and Failures specifies UPDATE or READ.

9. Tab down to Standard Access Permits and place an E next to it (hit enter)and

validate that UPDATE or higher access is limited to Systems Programming personnel

10. if CONDITIONAL ACCESS PERMITS: _ (E to edit data) has *data is present* next to it, place an E next to it and validate that conditional access

permits of Update or higher are limited to Systems Programming Personnel as well.

11. Repeat steps 2 through 10 for all datasets in option a.1

b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.

c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and alter access to program product data sets is limited to System Programmers 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 alter 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 IA0 to see that they are properly restricted to the ACP (Access Control Program) active on the system.

Data set prefix to be protected will be:

SYS2.TADZ.
 SYS2.TADZ.*.SHSIMOD1.** (optional fully-qualified APF).
 SYS3.TADZ.

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

```
ad 'sys2.TADZ.**' uacc(none) owner(sys2) -
  audit(success(update) failures(read)) -
  data('Vendor DS Profile: TADZ')
pe 'sys2.TADZ.**' id(syspauDt) acc(a)
pe 'sys2.tadz.**' id(audtaudt)
ad 'sys2.tadz.*.shsimod1.**' uacc(none) owner(sys2) -
  audit(success(update) failures(read)) -
  data('Vendor DS Profile: Tivoli Asset Discovery APF DS')
pe 'sys2.tadz.*.shsimod1.**' id(syspauDt) acc(a)
pe 'sys2.tadz.*.shsimod1.**' id(audtaudt)
ad 'sys3.TADZ.**' uacc(none) owner(sys3) -
  audit(success(update) failures(read)) -
  data('TADZ Vendor Datasets')
pe 'sys3.TADZ.**' id(syspauDt) acc(a)
pe 'sys3.tadz.**' id(audtaudt)
setr generic(dataset) refresh
```

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
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

Tivoli Asset Discovery for z/OS STC and/or batch data sets datasets, Likely:

1. hlq.TADZ.**

2. From the Administrator Main Menu choose Option 2 Security Server Commands

3. then choose Option: 3 Data Set

4. Type the resource names collected in option a.1 above into: Enter fully

qualified (without quotes) data set or profile name:

5. Hit enter.

6. Enter Y for Display covering profile? Y

7. Verify that the UACC is NONE

8. Verify that Audit Successes and Failures specifies UPDATE or READ.

9. Tab down to Standard Access Permits and place an E next to it (hit enter) and

validate that UPDATE or higher access is limited to Systems Programming Personnel. Verify that READ access is limited to job scheduling products and

System Auditors.

10. If CONDITIONAL ACCESS PERMITS: _ (E to edit data) has *data is present* next to it, place an E next to it and validate that conditional access

permits of UPDATE or higher are limited to Systems Programming Personnel. Verify that READ access is limited to job scheduling products and System Auditors.

11. Repeat steps 2 through 10 for all datasets in option a.1

b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.

c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and alter access to Tivoli Asset

Discovery for zOS (TADz) STC and/or batch data sets are limited to system programmers and TADz STC and/or batch jobs only.

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:

hlq.TADZ

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

```
ad 'hlq.tadz.*.iq*.*' uacc(none) owner(daztech) -
    audit(success(update) failures(read)) -
    data('TADZ Output Data')
ad 'hlq.tadz.*.uiq*.*' uacc(none) owner(daztech) -
    audit(success(update) failures(read)) -
    data('TADZ Output Data')
ad 'hlq.tadz.*.um*.*' uacc(none) owner(daztech) -
    audit(success(update) failures(read)) -
    data('TADZ Output Data')

pe 'hlq.tadz.*.iq*.*' id(syspauDt) acc(a)
pe 'hlq.tadz.*.iq*.*' id(tadzmon) acc(a)
pe 'hlq.tadz.*.iq*.*' id(tadziNq) acc(a)
pe 'hlq.tadz.*.uiq*.*' id(syspauDt) acc(a)
pe 'hlq.tadz.*.uiq*.*' id(tadzmon) acc(a)
pe 'hlq.tadz.*.uiq*.*' id(tadziNq) acc(a)
pe 'hlq.tadz.*.um*.*' id(syspauDt) acc(a)
pe 'hlq.tadz.*.um*.*' id(tadzmon) acc(a)
pe 'hlq.tadz.*.um*.*' id(tadziNq) acc(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

IACControls: ECCD-1, ECCD-2

Check Content:

a) Use Vanguard s Analyzer product to look at the Started Procedures Analysis report:

- a. From Analyzer main Menu, go to 3;4; Press <ENTER>
- b. Key in SORT PROCNAME; Press <ENTER>
- c. Key in L TADZMON; Press <ENTER>
- d. If not found then TADZMON; is not defined to RACF as a STC user.
- e. If found then you would use the U line command to determine if the userid is defined to RACF.
- f. Key the U line command for the TADZMON; entry; Press <ENTER>
- g. The userid is defined to RACF if a userid display appears. If not defined you should see the message Unable to display .

b) If the userid for the Tivoli Asset Discovery for z/OS started task is defined to the security database, there is NO FINDING.

c) If the userid for the Tivoli Asset Discovery for z/OS started task is not defined to the security database, this is a FINDING.

—

Fix Text: The Systems Programmer and IAO will ensure that the started task for TADz is properly defined.

Define the started task for TADz.

Example:

```
au tadzmon name('stc, tivoli AD') nopass -  
dfltgrp(stc) owner(stc) -  
data('stc for tivoli asset discovery')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-28561r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZTADR032
Rule Title: The Tivoli Asset Discovery for zOS (TADz) Started task is not 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
IACControls: ECCD-1, ECCD-2

Check Content:

a) Use Vanguard s Analyzer product to look at the Started Procedures Analysis report:

1. From Analyzer main Menu, go to 3;4; Press <ENTER>
2. Key in SORT PROCNAME; Press <ENTER>
3. Key in L TADZMON; Press <ENTER>
4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
5. If not found then TADZMON is not defined to RACF as a STC user.

b) If a STARTED resource class profile exists for the Tivoli Asset Discovery for z/OS started task TADZMON, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the Tivoli Asset Discovery for z/OS started task TADZMON, this is a FINDING.

Fix Text: Develop a plan to properly define and implement the userid(s) for each Tivoli Asset Discovery for zOS (TADz) Started Procedure.

A unique userid must be assigned for each NetView started task thru a corresponding STARTED class entry.

A sample set of commands is shown here:

```
rdef started tadzmon.** uacc(none) owner(admin) audit(all(read))
stdata(user(tadzmon) group(stc))
setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED