

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

UNCLASSIFIED

z/OS CA Auditor for RACF STIG

Version: 7

Release: 1

15 Mar 2025

XSL Release 5/15/2012 Sort by: STIGID

Description:

Group ID (Vulid): V-16932

Group Title: ZB000000

Rule ID: SV-31919r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZADTR000

Rule Title: CA Auditor installation data sets are not properly protected.

Vulnerability Discussion: CA Auditor 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

IAControls: 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 CA-Auditor Installation Datasets, Likely:

1. SYS2.IOA.*.CTD*.**
SYS3.IOA.*.CTDI.**
 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 step 1 above. This should be a fully qualified (without quotes) data set or profile name.
 5. Press ENTER
 6. Enter 'Y' for 'Display covering profile?' question
 7. Verify the UACC is NONE
 8. Verify that 'Audit Successes and Failures' specifies UPDATE or READ
 9. Tab to 'Standard Access Permits', place an E in this field, press ENTER and validate that UPDATE or higher access is limited to Systems Programming personnel. Verify READ access is restricted to auditors, security administrators, and/or CA Auditor's STCs and batch users.
 10. If 'CONDITIONAL ACCESS PERMITS: _ (E to edit data)' has *data is present* next to it, place an E next to it, press ENTER and validate that conditional access permits of UPDATE or higher are limited to Systems Programming Personnel as well. Verify READ access is restricted to auditors, security administrators, and/or CA Auditor's STCs and batch users.
 11. Repeat steps 2 through 10 for all datasets identified in step 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 CA Auditor installation data sets are limited to System Programmers only, and all update and alter access is logged. Read access can be given to auditors, security administrators, and/or CA Auditor s STCs and batch 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 alter 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.EXAMINE
SYS2A.EXAMINE

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

```
ad 'SYS2.EXAMINE.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('Vendor DS Profile: CA Auditor/Examine')
pe 'SYS2.EXAMINE.**' id(<syspautd>) acc(a)
pe 'SYS2.EXAMINE.**' id(<audtaudt> <secaudt> EXAMMON) acc(r)
ad 'SYS2A.EXAMINE.**' uacc(none) owner(sys2a) -
    audit(success(update) failures(read)) -
    data('Vendor DS Profile: CA Auditor/Examine')
pe 'SYS2A.EXAMINE.**' id(<syspautd>) acc(a)
pe 'SYS2A.EXAMINE.**' id(<audtaudt> <secaudt> EXAMMON) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid): V-21592

Group Title: ZB000002

Rule ID: SV-32206r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZADTR002

Rule Title: CA Auditor User data sets are not properly protected.

Vulnerability Discussion: CA Auditor User 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

IAControls: 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

CA-Auditor user data sets, Likely:

1. SYS3.EXAMINE
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. Tab down to Standard Access Permits and place an E next to it (hit enter) and validate that UPDATE, and/or ALTER access to systems programming personnel, security personnel and auditors.
 9. 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, and/or ALTER access to systems programming personnel, security personnel and auditors.
 10. Repeat steps 2 through 10 for all datasets in option a.1
- b) If a.7, a.8, and a.9 are all true, there is NO FINDING.
- c) If a.7, a.8, and a.9 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and alter access to CA Auditor User data sets are limited to System Programmers, security personnel and auditors.

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 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.EXAMINE

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

```
ad 'SYS3.EXAMINE.**' uacc(none) owner(sys3) -
    audit(failures(read)) -
    data('Vendor DS Profile: CA Auditor')
pe 'SYS3.EXAMINE.**' id(<syspautd>) acc(a)
pe 'SYS3.EXAMINE.**' id(<audtautd> <secautd>) acc(a)
```

```
setr generic(dataset) refresh
```

CCI: CCI-001499

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-32209r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZADTR020

Rule Title: CA Auditor resources are not properly defined and protected.

Vulnerability Discussion: CA Auditor can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to product resources could result in the compromise of the operating system environment, and compromise the confidentiality of customer data. Many utilities assign resource controls that can be granted to system programmers only in greater than read authority. Resources are also granted to certain non systems personnel with read only authority.

Responsibility: Information Assurance Officer

IAControls: ECCD-1, ECCD-2

Check Content:

Validate the following for the PROFILE LTDMMAIN resource in the PROGRAM resource

1. From the Administrator Main Menu Choose Option 3 Security Server Reports
2. then choose Option: 4 General Resource Profile
3. On the command line chose option 4 AND then Put (LTDMMAIN) next to PROFILE: and (PROGRAM) next to CLASS:
4. Hit enter.
5. Verify that the UACC for all profiles listed is NONE
6. Place an S next to the profile and validate that the access list is limited to sytem programmers, auditors and security personnel
If TYPE is GROUP, place an S in the CMD line
and hit enter to explode the GROUP.
7. For all resources with logging requirements place an LR next to the profile (hit enter and review the output) and validate that it specifies ALL(READ).

Fix Text: The IOA will verify that the LTDMMAIN resource in the PROGRAM resource class is restricted to sytem programmers, auditors and security personnel.

The RACF rules for the LTDMMAIN resource specify a default access of NONE

and no RACF rules that allow access to the LTDMMAIN resource.

Example:

```
rdef program LTDMMAIN uacc(none) owner(admin) audit(failure(read)) -  
data('added per PDI ZADT0020')
```

The RACF rules for the LTDMMAIN resource is restricted access to auditors and security personnel with access of READ. All RACF rules are defined with UACC(NONE).

Example:

```
rdef program ltdmmain -  
addmem('SYS2A.EXAMINE.V120SP01.CAILIB'//nopadchk) -  
data('Required by SRR PDI ZADTR020') -  
audit(all(read)) uacc(none) owner(admin)  
pe LTDMMAIN cl(program) id(syspauDt) acc(r)  
pe LTDMMAIN cl(program) id(audtauDt) acc(r)  
pe LTDMMAIN cl(program) id(secauDt) acc(r)  
  
setr when(program) ref
```

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED