

# **VANGUARD**

## **Integrity Professionals, Inc.**

---

**Enterprise Security Software**

z/OS CA Auditor for ACF2 STIG

Version: 6

Release: 3

29 Dec 2020

---

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

IACcontrols: 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:

- SENSITIVE.RPT(ADTRPT)

Automated Analysis

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

- PDI(ZADT0000)

Verify that the accesses to the CA Auditor installation data sets are properly restricted.

\_\_\_\_ The ACF2 data set rules for the data sets restricts READ access to

auditors, security administrators, and/or CA Auditor s STCs and batch users.

\_\_\_\_ The ACF2 data set rules for the data sets restricts UPDATE and/or ALTER access to systems programming personnel.

\_\_\_\_ The ACF2 data set rules for the data sets specify that all (i.e., failures and successes) UPDATE and/or ALTER access are logged.

Fix Text: The IAO will ensure that update and allocate access to CA Auditor installation data sets is limited to System Programmers only, and all update and allocate 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 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.EXAMINE

SYS2A.EXAMINE

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

\$KEY(SYS2)

EXAMINE.- UID(<syspau>) R(A) W(L) A(L) E(A)

EXAMINE.- UID(<audtaudt>) R(A) E(A)

EXAMINE.- UID(<secaudt>) R(A) E(A)

EXAMINE.- UID(EXAMMON) R(A) E(A)

\$KEY(SYS2A)

EXAMINE.- UID(<syspau>) R(A) W(L) A(L) E(A)

EXAMINE.- UID(<audtaudt>) R(A) E(A)  
EXAMINE.- UID(<secaudt>) R(A) E(A)  
EXAMINE.- UID(EXAMMON) R(A) E(A)

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 allocate 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 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.EXAMINE

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

\$KEY(SYS3)

EXAMINE.- UID(<syspau>) R(A) W(A) A(A) E(A)

EXAMINE.- UID(<audtaudt>) R(A) W(A) A(A) E(A)

EXAMINE.- UID(<secaudt>) R(A) W(A) A(A) E(A)

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

IACControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ZADT0020)
- ACF2CMDS.RPT(RESOURCE) Alternate report

#### Automated Analysis

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

- PDI(ZADT0020)

Verify that the access to the LTDMMAIN resource in the PROGRAM resource class is restricted.

\_\_\_ The ACF2 rules for the resources specify a default access of NONE.

\_\_\_ The ACF2 rules for the resources are restricted access to system programmers, auditors, and security personnel.

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

The ACF2 rules for the resource specify a default access of NONE. There are ACF2 rules defined and only system programmers, auditors, and security personnel have access.

Example:

```
SET R(PGM)
$KEY(LTDMMAIN) TYPE(PGM)
  UID(<syspaut>) ALLOW
  UID(<audtaut>) ALLOW
  UID(<secaudt>) ALLOW
  UID(*) PREVENT DATA(SRR FINDING FOR CA AUDITOR)
```

CCI: CCI-000035

CCI: CCI-002234

---

UNCLASSIFIED