

# **VANGUARD**

**Integrity Professionals, Inc.**

---

**Enterprise Security Software**

z/OS ROSCOE for ACF2 STIG

Version: 6

Release: 7

29 Dec 2020

---

Group ID (Vulid): V-16932  
Group Title: ZB000000  
Rule ID: SV-21927r2\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZROSR000  
Rule Title: ROSCOE Install data sets are not properly protected.

Vulnerability Discussion: ROSCOE 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  
IAControls: 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(ROSRPT)

Automated Analysis

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

- PDI(ZROS0000)

b) Verify that access to the ROSCOE 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. Security Personnel and 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.ROSCOE  
SYS2A.ROSCOE  
SYS3.ROSCOE  
SYS3A.ROSCOE

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

\$KEY(SYS2)  
ROSCOE.- UID(syspautd) R(A) W(L) A(L) E(A)  
ROSCOE.- UID(secaudt) R(A) E(A)  
ROSCOE.- UID(audtaudt) R(A) E(A)

\$KEY(SYS2A)  
ROSCOE.- UID(syspautd) R(A) W(L) A(L) E(A)  
ROSCOE.- UID(secaudt) R(A) E(A)  
ROSCOE.- UID(audtaudt) R(A) E(A)

\$KEY(SYS3)  
ROSCOE.- UID(syspautd) R(A) W(L) A(L) E(A)  
ROSCOE.- UID(secaudt) R(A) E(A)  
ROSCOE.- UID(audtaudt) R(A) E(A)

\$KEY(SYS3A)  
ROSCOE.- UID(syspautd) R(A) W(L) A(L) E(A)  
ROSCOE.- UID(secaudt) R(A) E(A)  
ROSCOE.- UID(audtaudt) R(A) E(A)

CCI: CCI-000213

CCI: CCI-002234

---

Group ID (Vulid): V-17067  
Group Title: ZB000001  
Rule ID: SV-23706r2\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZROSR001  
Rule Title: ROSCOE STC data sets are not properly protected.

Vulnerability Discussion: ROSCOE STC 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:

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

- SENSITIVE.RPT(ROSSTC)

Automated Analysis

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

- PDI(ZROS0001)

b) Verify that access to the ROSCOE STC data sets are properly restricted. The data sets in this group are the data sets identified in the ROSACTxx (if used), ROSLIBxx, and SYSAWSx DD statements of the STC or batch JCL.

\_\_\_ 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 restrict UPDATE and/or ALTER access to the product STC(s) and/or batch job(s).

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 the ROSCOE started task or batch job data sets is limited to system programmers and the started task only and all update and allocate access is logged.

The IAO will ensure that all other accesses to the ROSCOE started task or batch job data sets are properly restricted and all required accesses are properly logged.

Data sets to be protected will be

SYS3.ROSCOE.SYS\*\*

SYS3.ROSCOE.ROSLIB\*\*

Example:

```
SET RULE
$KEY(SYS3)
ROSCOE.SYS- UID(syspu dt) R(A) W(L) A(L) E(A)
ROSCOE.SYS- UID(stc roscoe) R(A) W(L) A(L) E(A)
ROSCOE.ROSLIB- UID(syspu dt) R(A) W(L) A(L) E(A)
ROSCOE.ROSLIB- UID(stc roscoe) R(A) W(L) A(L) E(A)
```

CCI: CCI-001499

---

Group ID (Vulid): V-17947  
Group Title: ZB000020  
Rule ID: SV-23708r2\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZROS020  
Rule Title: ROSCOE resources are not properly defined and protected.

Vulnerability Discussion: ROSCOE can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to program 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:

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

- SENSITVE.RPT(ZROS0020)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

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

- PDI(ZROS0020)

Ensure that all ROSCOE resources and/or generic equivalent are properly protected according to the requirements specified in CA ROSCOE Resources table

in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

\_\_\_ The ACF2 resources are defined with a default access of PREVENT.

\_\_\_ The ACF2 resource access authorizations restrict access to the appropriate personnel.

\_\_\_ The ACF2 resource logging is correctly specified.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Ensure that all ROSCOE resources and/or generic equivalent are properly protected according to the requirements specified in CA ROSCOE Resources table in the z/OS STIG Addendum.

Use CA ROSCOE Resources table in the z/OS STIG Addendum. This table lists the resources, access requirements, and logging requirements for ROSCOE ensure the following guidelines are followed:

The ACF2 resources are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel.

The ACF2 resource logging is correctly specified.

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

```
$KEY(rosid) TYPE(ROS)
ROSCMD.ETSO UID(*) SEVICE(READ)
ROSCMD.MONITOR.- UID(syspautd) ALLOW
ROSCMD.MONITOR.AMS UID(syspautd) ALLOW
ROSCMD.MONITOR.AMS UID(*) SEVICE(READ)
ROSCMD.- UID(syspautd) ALLOW
- UID(*) PREVENT
```

CCI: CCI-000035

CCI: CCI-002234

---

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-28585r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZROSR030

Rule Title: ROSCOE Started Task name 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) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(LOGONIDS)

b) Ensure the following fields are completed for each STC logonid for the product:

STC  
JOBFROM  
MUSASS  
NO-SMC

c) Ensure the following fields are completed for each Batch logonid for the product:

JOB  
JOBFROM  
MUSASS  
NO-SMC

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

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

Fix Text: The ROSCOE system programmer and the IAO 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 ROSCOE JOBFROM MUSASS NO-SMC

CCI: CCI-000764

---

Group ID (Vulid): V-18011  
Group Title: ZB000038  
Rule ID: SV-24846r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZROSR038  
Rule Title: The Product's Resource Class for Roscoe is not defined or active in the ACP.

Vulnerability Discussion: Failure to use a robust ACP to control a product could potentially compromise the integrity and availability of the MVS operating system and user data.

Responsibility: Information Assurance Officer  
IAControls: DCCS-1, DCCS-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ACFGSO)

b) Ensure that the following GSO CLASMAP record entries are defined:

CLASMAPqual RESOURCE(ROSRES) RSRCTYPE(ROS)

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: The IAO will use SAF security to define and protect the Products resource class(es).



Ensure that the following GSO CLASMAP record entry(ies) is (are) defined:

CLASMAP.ROSCOE ENTITYLN(39) RESOURCE(ROSRES) RSRCTYPE(ROS)

Example:

```
SET C(GSO)
LIST CLASMAP.ROSCOE
INSERT CLASMAP.ROSCOE ENTITYLN(39) RESOURCE(ROSRES) RSRCTYPE(ROS)
```

F ACF2,REFRESH(CLASMAP)

CCI: CCI-000336

CCI: CCI-002358

---

Group ID (Vulid): V-18014

Group Title: ZB000040

Rule ID: SV-23712r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZROSR040

Rule Title: Product configuration/parameter values are not specified properly.

Vulnerability Discussion: Product configuration/parameters control the security and operational characteristics of products. If these parameter values are improperly specified, security and operational controls may be weakened. This exposure may threaten the availability of the product applications, and compromise the confidentiality of customer data.

Responsibility: Systems Programmer

IAControls: ECCD-1, ECCD-2

Check Content:

The following steps are necessary for reviewing the ROSCOE options:

- a) Have the products system programmer display the configuration/parameters control statements used in the current running product to define or enable security. This information is located in the SYSIN DD statement in the JCL of the STC Batch job.
- b) Verify the following specifications:

Keyword Value

EXTSEC RACF

ACFEXT YES  
CLLEXT YES  
JOBEXT YES  
LIBEXT YES  
MONEXT YES  
PRVEXT YES  
RPFEXT YES  
UPSEXT YES

c) If (b) above is true, there is NO FINDING.

d) If (b) above is untrue, this is a FINDING

---

Fix Text: The product systems programmer will verify that any configuration / parameters that are required to control the security of the product are properly configured and syntactically correct.

See the required parameters below: Example

Keyword	Value
EXTSEC	ACF2
ACFEXT	YES
CLLEXT	YES
JOBEXT	YES
LIBEXT	YES
MONEXT	YES
PRVEXT	YES
RPFEXT	YES
UPSEXT	YES

CCI: CCI-000035

---

UNCLASSIFIED