VANGUARD
INTEGRITY PROFESSIONALS
INFORMATION SECURITY EXPERTS

z/OS ROSCOE for RACF STIG

Version: 6

Release: 8

30 June 2023

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

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) Check with your IOA or Systems Programming personnel and compile the list of
ROSCOE Installation Datasets, Likely:
1. hlq.ROSCOE.**
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, Security Personnel and Auditors only, and all update and allocate access is logged.

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 IAO 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.ROSCOE.
SYS2A.ROSCOE.
SYS3.ROSCOE.
SYS3A.ROSCOE.

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

```
ad 'sys2.roscoe.**' uacc(none) owner(sys2) -
       audit(success(update) failures(read)) -
      data('Vendor DS Profile: ROSCOE')
pe 'sys2.roscoe.**' id(syspaudt) acc(a)
pe 'sys2.roscoe.**' id(*) acc(r)
ad 'sys2a.roscoe.**' uacc(none) owner(sys2a) -
       audit(success(update) failures(read)) -
      data('Roscoe Vendor Datasets')
pe 'sys2a.roscoe.**' id(<syspaudt>) acc(a)
pe 'sys2a.roscoe.**' id(*) acc(r)
ad 'sys3.roscoe.**' uacc(none) owner(sys3) -
       audit(success(update) failures(read)) -
      data('Roscoe Vendor Datasets')
pe 'sys3.roscoe.**' id(<syspaudt>) acc(a)
pe 'sys3.roscoe.**' id(*) acc(r)
ad 'sys3a.roscoe.**' uacc(none) owner(sys3a) -
       audit(success(update) failures(read)) -
      data('Roscoe Vendor Datasets')
pe 'sys3a.roscoe.**' id(<syspaudt>) acc(a)
pe 'sys3a.roscoe.**' id(*) acc(r)
setr generic(dataset) refresh
```

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) Check with your IOA or Systems Programming personnel and compile the list of ROSCOE STC datasets, Likely:
1. hlq.ROSCOE.sys*.**
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 the ROSCOE started task or batch job data sets is limited to system programmers and the started task only and all update and alter 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.ros*.**

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

```
ad 'sys3.roscoe.ros*.**' uacc(none) owner(sys3) -
       audit(success(update) failures(read)) -
      data('Site Customized Profile: ROSCOE')
pe 'sys3.roscoe.ros*.**' id(syspaudt) acc(a)
pe 'sys3.roscoe.ros*.**' id(roscoe) acc(a)
ad 'sys3.roscoe.sys*.**' uacc(none) owner(sys3) -
       audit(success(update) failures(read)) -
      data('Site Customized profile: ROSCOE')
pe 'sys3.roscoe.sys*.**' id(syspaudt) acc(a)
pe 'sys3.roscoe.sys*.**' id(roscoe) acc(a)
setr generic(dataset) refresh
```

CCI: CCI-001499

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-23708r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZROSR020
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:

a) Refer to the CA ROSCOE Resources table, in the z/OS STIG Addendum.
Ensure
that
all items in #4 are true for each resource:
1. From the Administrator Main Menu choose Option 3 Security Server
Reports
2. Then choose Option: 4 General Resource Profile
3. Next to CLASS type in RO@RES and hit enter
4. Review each resource :
a. Verify that each UACC is NONE.
b. Verify the resource is defined.
c. Enter 'LV' or 'LR' next to each resource name
 - Verify that 'WARNING" is NO.
 - Verify that access to each resource is restricted to Appropriate
 Personnel as defined in the table referenced above in the z/OS STIG
Addendum.
 - 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
 - Tab down to Conditional Access Permits and validate that conditional
 access permits of Update or higher are limited to Systems
 Programming Personnel as well.
 - Verify that Audit settings are per the CA ROSCOE Resources table
 - Repeat step 4a-c, for all resources in CA ROSCOE Resources table.

b) If All items in step 4 are true, there is NO FINDING.

c) If any item in step 4 is not true, this is a FINDING.

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

1) The ROSCOE Resources are properly defined and proper access is
restricted
according to the CA ROSCOE Resources table, in the z/OS STIG Addendum.

2) Verify that logging is specified according to the CA ROSCOE Resources
table,
in the z/OS STIG Addendum

The systems programmer will see that the questionaire member for this
product
vulnerability contains the resources, authorized users access levels and
logging
requirements, based on the sites requirements.

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
IAControls: ECCD-1, ECCD-2

Check Content:

a) Use Vanguard s Analyzer product to look at the Started Procedures
Analysis
report: Do the following for the ROSCOE started task, likely called
ROSCOE

a. From Analyzer main Menu, go to 3;4; Press <ENTER>
b. Key in SORT PROCNAME; Press <ENTER>
c. Key in L ROSCOE; Press <ENTER>
d. If not found then ROSCOE is not defined to RACF as a STC user.
e. If found but has a R in the M column, review the message and ensure
that
the following does not appear: VSA346R The user ID does not have the
protected attribute. If message exists, then user does not have the
PROTECTED attribute. This is a finding.
f. If found then you would use the U line command to determine if the
userid is defined to RACF.
g. Key the U line command for the ROSCOE entry; Press <ENTER>
h. 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 ROSCOE started task is defined to the security
database

with the PROTECTED attribute, there is NO FINDING.

c) If the userid for the ROSCOE started task is not defined to the security database or does not have the PROTECTED attribute, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (3)

Fix Text: The ROSCOE system programer 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 Statrted 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.

A sample is provided here:

```
au roscoe name('stc, roscoe') owner(stc) dfltgrp(stc) nopass
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-24812r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZROSR032
Rule Title: The ROSCOE 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.

This vulnerability will be used for both RACF and Top Secret. ACF2 does not required for this check

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

Check Content:

Use Vanguard s Analyzer product to look at the Started Procedures Analysis report: The name of the roscoe started task is likely ROSCOE.

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

b) If a STARTED resource class profile exists for the started task ROSCOE, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the started task for ROSCOE, this is a FINDING.

___

Fix Text: Develop a plan to properly define and implement the userid(s) for each ROSCOE Started Procedure.

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

A sample set of commands is shown here:

```
rdef started roscoe.** uacc(none) owner(admin) audit(all(read))
stdata(user(=member) group(stc))
```

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:

Use Vanguard s Administrator product Validate that CLASS RO@RES is active.

a) From Administrator main menu, select Security Server Commands,

b) Press <ENTER>

c) Select SETROPTS option 5 SETROPTS option,

d) Press <ENTER>

e) On the SETROPTs screen, locate the CDT Classes prompt, enter E next to it.

f) Press <ENTER>

g) Invoke the locate command, Locate RO@RES

h) Screen print the display showing the attributes of the RO@RES class, including active status
1. If the RO@RES class is ACTIVE there is NOFINDING
2. If the RO@RES class is not ACTIVE there is a FINDING

___

Fix Text: The IAO will ensure that the Product Resource Class(es) is (are) active.

Issue the following commands:

```
SETR CLASSACT(RO@RES)
SETR GENERIC(RO@RES)
```

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

CCI: CCI-000035

____

UNCLASSIFIED