

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS ROSCOE for TSS STIG

Version: 6

Release: 7

20 Jan 2015

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-21902r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZROST000
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.

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 TSS data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

___ The TSS 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/create access to program product data sets is limited to System Programmers only, and all update and allocate/create 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 allocate/create access and if required that all update and allocate/create 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:

TSS PERMIT(syspautd) DSN(SYS2.ROSCOE.) ACCESS(R)
TSS PERMIT(syspautd) DSN(SYS2.ROSCOE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(secapautd) DSN(SYS2.ROSCOE.) ACCESS(R)
TSS PERMIT(audtautd) DSN(SYS2.ROSCOE.) ACCESS(R)

TSS PERMIT(syspautd) DSN(SYS2A.ROSCOE.) ACCESS(R)
TSS PERMIT(syspautd) DSN(SYS2A.ROSCOE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(secapautd) DSN(SYS2A.ROSCOE.) ACCESS(R)
TSS PERMIT(audtautd) DSN(SYS2A.ROSCOE.) ACCESS(R)

TSS PERMIT(syspautd) DSN(SYS3.ROSCOE.) ACCESS(R)
TSS PERMIT(syspautd) DSN(SYS3.ROSCOE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(secapautd) DSN(SYS3.ROSCOE.) ACCESS(R)
TSS PERMIT(audtautd) DSN(SYS3.ROSCOE.) ACCESS(R)

TSS PERMIT(syspautd) DSN(SYS3A.ROSCOE.) ACCESS(R)
TSS PERMIT(syspautd) DSN(SYS3A.ROSCOE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(secapautd) DSN(SYS3A.ROSCOE.) ACCESS(R)
TSS PERMIT(audtautd) DSN(SYS3A.ROSCOE.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-23707r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZROST001
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.

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 TSS data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

____ The TSS 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/create 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/create 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**

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

```
TSS ADD(SYS3) DSN(SYS3)
TSS PER(syspau dt) DSN(SYS3.ROSCOE.SYS) ACC(R)
TSS PER(syspau dt) DSN(SYS3.ROSCOE.SYS) ACC(A) ACTION(AUDIT)
TSS PER(roscoe stc) DSN(SYS3.ROSCOE.SYS) ACC(R)
TSS PER(roscoe stc) DSN(SYS3.ROSCOE.SYS) ACC(A) ACTION(AUDIT)
TSS PER(syspau dt) DSN(SYS3.ROSCOE.ROSLIB) ACC(R)
TSS PER(syspau dt) DSN(SYS3.ROSCOE.ROSLIB) ACC(A) ACTION(AUDIT)
TSS PER(roscoe stc) DSN(SYS3.ROSCOE.ROSLIB) ACC(R)
TSS PER(roscoe stc) DSN(SYS3.ROSCOE.ROSLIB) ACC(A) ACTION(AUDIT)
```

CCI: CCI-001499

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-23709r3_rule

Severity: CAT II

Rule Version (STIG-ID): ZROST020

Rule Title: ROSCOE resources must be 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 product resources could result in the compromise of the operating system environment, and compromise the confidentiality and integrity 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.

IAControls: ECCD-1, ECCD-2

Check Content:

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

- SENSITVE.RPT(ZROS0020)

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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

____ The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

____ The TSS resource logging is specified as designated in the above table.

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

(Note: The resources and/or resource prefixes identified below are examples of a possible installation. The actual 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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The TSS resource logging is specified as designated in the above table.

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

```
TSS ADD(dept-acid) ROSRES(rosid)
TSS PERMIT(ALL) ROSRES(rosid.ROSCMD.ETSO) ACCESS(READ)
TSS PERMIT(syspautd) ROSRES(rosid.ROSCMD.MONITOR.) ACCESS(ALL)
TSS PERMIT(syspautd) ROSRES(rosid.ROSCMD.MONITOR.AMS) ACCESS(ALL)
TSS PERMIT(ALL) ROSRES(rosid.ROSCMD.MONITOR.AMS) ACCESS(READ)
TSS PERMIT(syspautd) ROSRES(rosid.ROSCMD.) ACCESS(ALL)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-23711r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZROST030

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.

IAControls: ECCD-1, ECCD-2

Check Content:

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

- TSSCMDS.RPT(@ACIDS)

b) Review each ROSCOE STC/Batch ACID(s) for the following:

___ Is defined with Facility of STC and/or BATCH.

___ Is defined with Master Facility of ROSCOE.

___ Is sourced to the INTRDR.

c) If all of the above are true, there is NO FINDING.

d) If any of the above is untrue, 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.

A sample is provided here:

```
TSS CREATE(ROSCOE) TYPE(USER) -  
    NAME('*STC* for ROSCO') DEPT(XXXX) -  
FAC(STC) -  
    MASTFAC(ROSCOE) PASS(XXXXXXXX,0) -  
    SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

Group ID (Vulid): V-17454

Group Title: ZB000032

Rule ID: SV-24813r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZROST032

Rule Title: ROSCOE Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.

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.

IAControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(#STC)

Automated Analysis

Refer to the following report produced by the TSS Data Collection:

- PDI(ZROS0032)

Verify that the ROSCOE started task(s) is (are) defined in the TSS STC record.

Fix Text: The ROSCOE system programmer and the IAO will ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the ROSCOE started task(s) thru a corresponding STC table entry.

The following sample set of commands is shown here as a guideline:

TSS ADD(STC) PROCNAME(ROSCOE) ACID(ROSCOE)

CCI: CCI-000764

Group ID (Vulid): V-17469

Group Title: ZB000036

Rule ID: SV-24943r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZROST036

Rule Title: ROSCOE is not properly defined to the Facility Matrix Table for Top Secret.

Vulnerability Discussion: Improperly defined security controls for the Product could result in the compromise of the network, operating system, and customer data.

*****This vulnerability only applies to Top Secret started tasks. *****

IAControls: ECCD-1, ECCD-2

Check Content:

a) Refer to the following reports produced by the TSS Data Collection:

- TSSCMDS.RPT(FACLIST) - Preferred report containing all control option values in effect including default values.
- TSSCMDS.RPT(TSSPRMFL) - Alternate report containing only control option values explicitly coded at TSS startup.

NOTE: The FACLIST report must be created by DECC security personnel. The TSSPRMFL report can be used if DECC security personnel have not executed the required steps documented in the TSS Data Collection.

b) Review the FACLIST report. Ensure the Product Facility is properly defined as specified by the product system programmer.

c) If the Product facility control options are defined as indicated by the product system programmer, there is NO FINDING.

d) If any of the Product facility control options are not defined as indicated by the product system programmer, this is a FINDING.

Fix Text: The Facility ROSCOE comes predefined with CA-TSS. Please ensure you add the following to your TSS parmlib for the FAC(ROSCOE):

**** ROSCOE *

FACILITY(ROSCOE=NOLUMSG,NORNDPW)

CCI: CCI-000764

Group ID (Vulid): V-18011

Group Title: ZB000038

Rule ID: SV-24847r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZROST038

Rule Title: Resouce Class ROSRES 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.

IAControls: DCCS-1, DCCS-2

Check Content:

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

- TSSCMD5.RPT(#RDT)

b) Ensure that Product Resource Class(es) is (are) defined in the Resource Definition Table as follows:

Note: Identify all of the attributes and characteristics of the Product resource class in the TSS Resource Definition Table (delete this note).

RESOURCE CLASS = ROSRES

RESOURCE CODE = X'hex code'

ATTRIBUTE = MASK|NOMASK,MAXOWN(08),MAXPERMIT(044),ACCESS,DEFPROT

ACCESS = NONE(0000),CONTROL(0400),UPDATE(6000),READ(4000)

ACCESS = WRITE(2000),ALL(FFFF)

DEFACC = READ

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 ensure the Product resource class(es) is (are) defined in the TSS RDT. The IAO will issue one of the following commands to define the Product resource class(es):

TSS REPLACE(RDT) RESCLASS(ROSRES) -
MAXLEN(044) -
ATTR(MASK|NOMASK,DEFPROT) -
ACLST(NONE(0000),CONTROL(0400),UPDATE(6000),READ(4000),WRITE(2000),ALL(FFFF)) -
DEFACC(READ)

TSS ADDTO(RDT) RESCLASS(ROSRES) -
RESCODE(hex-code) -
ATTR(MASK|NOMASK,DEFPROT) -
ACLST(NONE(0000),CONTROL(0400),UPDATE(6000),READ(4000),WRITE(2000),ALL(FFFF)) -
DEFACC(READ)

CCI: CCI-002358

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-23714r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZROST040
Rule Title: ROSCOE 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.

IAControls: ECCD-1, ECCD-2

Check Content:

a) Have the the product system programmer display the configuration/parameter 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.

Automated Analysis

Refer to the following report produced by the z/OS Data Collection:

- PDI(ZROS0040)

b) Verify the following specifications:

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

CCI: CCI-000035

UNCLASSIFIED