VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS SRRAUDIT for TSS STIG

Version: 6

Release: 4

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-21731r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZSRRT000
Rule Title: SRRAUDIT installation data sets must be properly protected.

Vulnerability Discussion: SRRAUDIT 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.

IAControls: 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:

- SENSITVE.RPT(SRRPROD)

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

- PDI(ZSRR0000)

Verify that the accesses to the SRRAUDIT installation data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS data set access authorizations restricts READ access to systems programming personnel, domain level production control and scheduling personnel, security personnel, and auditors.

___ The TSS data set access authorizations restricts WRITE and/or greater access to systems programming personnel.

___ The TSS data set access authorizations specify that all (i.e., failures and successes) WRITE and/or greater accesses are logged.

Fix Text: The IAO will ensure WRITE and/or greater access to SRRAUDIT installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. All failures and successful WRITE and/or greater accesses are logged.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have WRITE and/or greater access and, if required, that all WRITE and/or greater accesses are logged. He will identify if any additional groups have WRITE and/or greater 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.

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

Data sets to be protected will be:
SYS2.SRRAUDIT.

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

```
TSS PERMIT(syspaudt) DSN(SYS2.SRRAUDIT.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS2.SRRAUDIT.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(tstcaudt) DSN(SYS2.SRRAUDIT.) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS2.SRRAUDIT.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(audtaudt) DSN(SYS2.SRRAUDIT.) ACCESS(R)
TSS PERMIT(pcspaudt) DSN(SYS2.SRRAUDIT.) ACCESS(R)
TSS PERMIT(secaaudt) DSN(SYS2.SRRAUDIT.) ACCESS(R)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-23905r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSRRT002
Rule Title: SRRAUDIT User data sets are not properly protected.

Vulnerability Discussion: SRRAUDIT User 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:

- SENSITVE.RPT(SRRUSER)

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

- PDI(ZSRR0002)

b) Verify that access to the SRRAUDIT User data sets are properly restricted.

___ The TSS data set rules for the data sets does not restrict READ, UPDATE, and/or ALTER access to systems programming personnel, security personnel, and auditors.

___ The TSS data set rules for the data sets do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

b) If all of the above are untrue, there is NO FINDING.

c) If any of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that read, update, and allocate access to program product user data sets is limited to System Programmers, Security Personnel, and Auditors and all update and allocate access is logged.

The installing System Programmer will identify and document the product user data sets and categorize them according to who will have update and allocate 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 set prefix to be protected will be:

SYS3.SRRAUDIT.

If doing a full SRR review using the z/OS STIG Instruction, the following data set prefix to be protected will be:

SYS3.FSO.

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

```
TSS ADD(SYS3) DSN(SYS3)
TSS PER(syspaudt) DSN(SYS3.SRRAUDIT.) ACC(R)
TSS PER(secaaudt) DSN(SYS3.SRRAUDIT.) ACC(R)
TSS PER(audtaudt) DSN(SYS3.SRRAUDIT.) ACC(R)
TSS PER(syspaudt) DSN(SYS3.SRRAUDIT.) ACC(A) ACTION(AUDIT)
TSS PER(secaaudt) DSN(SYS3.SRRAUDIT.) ACC(A) ACTION(AUDIT)
TSS PER(audtaudt) DSN(SYS3.SRRAUDIT.) ACC(A) ACTION(AUDIT)

TSS PER(syspaudt) DSN(SYS3.FSO.) ACC(R)
TSS PER(secaaudt) DSN(SYS3.FSO.) ACC(R)
TSS PER(audtaudt) DSN(SYS3.FSO.) ACC(R)
TSS PER(syspaudt) DSN(SYS3.FSO.) ACC(A) ACTION(AUDIT)
TSS PER(secaaudt) DSN(SYS3.FSO.) ACC(A) ACTION(AUDIT)
TSS PER(audtaudt) DSN(SYS3.FSO.) ACC(A) ACTION(AUDIT)
```

CCI: CCI-001499

UNCLASSIFIED