VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS CA Auditor for TSS STIG

Version: 6

Release: 3

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-31920r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZADTT000
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.

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(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 TSS data set rules for the data sets restricts READ access to auditors, security administrators, and/or CA Auditor's STCs and batch users.

___ The TSS data set rules for the data sets restricts UPDATE and/or ALL access to systems programming personnel.

___ The TSS data set rules for the data sets specify that all (i.e., failures and successes) UPDATE and/or ALL 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:

TSS PERMIT(<syspaudt>) DSN(SYS2.EXAMINE.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2.EXAMINE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.EXAMINE.) ACCESS(R)
TSS PERMIT(<secaaudt>) DSN(SYS2.EXAMINE.) ACCESS(R)
TSS PERMIT(EXAMMON) DSN(SYS2.EXAMINE.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2A.EXAMINE.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2A.EXAMINE.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2A.EXAMINE.) ACCESS(R)
TSS PERMIT(<secaaudt>) DSN(SYS2A.EXAMINE.) ACCESS(R)
TSS PERMIT(EXAMMON) DSN(SYS2A.EXAMINE.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-32207r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZADTT002
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.

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(ADTUSER)

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

- PDI(ZADT0002)

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

___ The TSS data set rules for the data sets restricts UPDATE and/or ALL access to systems programming personnel, security personnel and auditors.

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:

TSS PERMIT(<syspaudt>) DSN(SYS3.EXAMINE) ACCESS(ALL)
TSS PERMIT(<audtaudt>) DSN(SYS3.EXAMINE) ACCESS(ALL)
TSS PERMIT(<secaaudt>) DSN(SYS3.EXAMINE) ACCESS(ALL)

CCI: CCI-001499

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-32210r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZADTT020
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.

IAControls: ECCD-1, ECCD-2

Check Content:
Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(ZADT0020)

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 TSS owner is defined for the prefix of the resource and/or the resource classes RDT entry has DEFPROT specified.

___ The TSS 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 TSS owner is defined for the LTDMMAIN resource and/or PROGRAM RDT entry has DEFPROT specified.

Example:

TSS ADD(dept-acid)PROGRAM(LTDMMAIN)

TSS REP(RDT)RESCLASS(PROGRAM)ATTR(DEFPROT)

The TSS rules for the LTDMMAIN resource is restricted access to system programmers, auditors, and security personnel.

Example:

TSS PERMIT(audtaudt)PROGRAM(LTDMMAIN)
TSS PERMIT(secaaudt)PROGRAM(LTDMMAIN)
TSS PERMIT(syspaudt)PROGRAM(LTDMMAIN)

CCI: CCI-000035

CCI: CCI-002234
