z/OS Compuware Abend-AID for TSS STIG

Version: 6

Release: 6

27 Jul 2018

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-43205r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZAID0040
Rule Title: Compuware Abend-AID external security options must be specified properly.

Vulnerability Discussion: Compuware Abend-AID offers external security interfaces that are controlled by parameters specified in FDBDPARM DD statement of the started task procedures. These interfaces provide security controls for Abend-AID. Without proper controls to ensure that security is active, the integrity of the Compuware Abend-AID System and the confidentiality of data stored on the system may be compromised.

Check Content:
Examine the Enterprise Common Components (ECC) started task procedure. (This can usually be found in the system PROCLIBs). Refer to the contents of the data set specified in the CWPARM DD statement.

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

- PDI(ZAID0040)

Review the Member name listed.

If the following is specified for each component, this is not a finding.
Member Name: AABD00 - Abend-AID batch dump capture address space
EXTERNAL_SECURITY_ENABLED=YES
Member Name: AATD00 - Abend-AID CICS Transaction Dump Capture Address Space
EXTERNAL_SECURITY_ENABLED=YES
Member Name: AAVW00 - Abend-AID viewing server
EXTERNAL_SECURITY_ENABLED=YES

Fix Text: In the data set specified in the CWPARM DD statement from the ECC started task procedure, specify the parameter values for each component in the respective members as follows:

Member Name: AABD00 - Abend-AID batch dump capture address space
EXTERNAL_SECURITY_ENABLED=YES
Member Name: AATD00 - Abend-AID CICS Transaction Dump Capture Address Space
EXTERNAL_SECURITY_ENABLED=YES

Member Name: AAVW00 - Abend-AID viewing server
EXTERNAL_SECURITY_ENABLED=YES

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-43167r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDT000
Rule Title: Compuware Abend-AID installation data sets will be properly protected.

Vulnerability Discussion: Compuware Abend-AID 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.

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

- SENSITVE.RPT(AIDRPT)

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

- PDI(ZAID0000)

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

___ The TSS data set rules for the data sets restricts READ access to all authorized users.

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

___ The TSS data set rules for the data sets specify that all (i.e., failures and successes) WRITE and/or greater access is logged.

Fix Text: The IAO will ensure that WRITE and/or greater access to Compuware

Abend-AID installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to all authorized users.

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 access is 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.

Data sets to be protected will be:
SYS2.ABENDAID.
SYS2A.ABENDAID.
SYS3A.ABENDAID.

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

TSS ADD(SYS2) DSN(SYS2)
TSS ADD(SYS2A) DSN(SYS2A)
TSS ADD(SYS3A) DSN(SYS3A)
TSS PERMIT(syspaudt) DSN(SYS2.ABENDAID.V) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS2.ABENDAID.V) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS2.ABENDAID.V) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS2A.ABENDAID.V) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS2A.ABENDAID.V) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS2A.ABENDAID.V) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS3A.ABENDAID.V) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS3A.ABENDAID.V) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS3A.ABENDAID.V) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-43170r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDT001
Rule Title: Compuware Abend-AID STC data sets will be properly protected.

Vulnerability Discussion: Compuware Abend-AID STC 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.

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

- SENSITVE.RPT(AIDSTC)

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

- PDI(ZAID0001)

Verify that the accesses to the Compuware Abend-AID STC data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS data set rules for the data sets restricts READ access to auditors.

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

___ The TSS data set rules for the data sets restricts WRITE and/or greater access to the Compuware Abend-AID's STC(s) and/or batch user(s).

Fix Text: The IAO will ensure that WRITE and/or greater access to Compuware Abend-AID STC data sets is limited to System Programmers and/or Compuware Abend-AID's STC(s) and/or batch user(s) only. READ access can be given to auditors.

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 access is 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.

Data sets to be protected will be:
SYS3.ABENDAID.

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

TSS ADD(SYS3) DSN(SYS3)

TSS PERMIT(syspaudt) DSN(SYS3.ABENDAID.) ACCESS(ALL)
TSS PERMIT(ABEND-AID STCs) DSN(SYS3.ABENDAID.) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(SYS3.ABENDAID) ACCESS(READ)

CCI: CCI-001499

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-75841r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDT002
Rule Title: Compuware Abend-AID user data sets must be properly protected.

Vulnerability Discussion: Compuware Abend-AID 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.

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

- SENSITVE.RPT(AIDUSER)

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

- PDI(ZAID0002)

Verify that the accesses to the following Compuware Abend-AID user data sets are properly restricted:
Region dump datasets
Report databases
Source listing files/source listing shared directories

If the following guidance is true, this is not a finding.

___ The TSS data set rules for the listed data sets restricts READ access to auditors.

___ The TSS data set rules for the listed data sets restricts WRITE and/or greater access to systems programming personnel.

___ The TSS data set rules for the listed data sets restricts WRITE and/or greater access to the Compuware Abend-AID's STC(s) and/or batch user(s).

___ The TSS data set rules for the listed data sets restricts CONTROL access to Application Development Programmers and Application Production Support Team members.

Fix Text: Ensure that WRITE and/or greater access to Compuware Abend-AID User data sets listed is limited to System Programmers and Compuware Abend-AID's STC(s) and/or batch user(s) only. Ensure that CONTROL access to Compuware Abend-AID User data sets listed is limited to Application Development Programmers and Application Production Support Team members. READ access can be given to auditors.

(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:
Region dump datasets
Report databases
Source listing files/source listing shared directories

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

TSS ADD(SYS3) DSN(SYS3.)

TSS PERMIT(syspaudt) DSN(SYS3.ABENDAID.REPORTDB) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.ABENDAID.REPORTDB) ACCESS(ALL)
TSS PERMIT(ABEND-AID STCs) DSN(SYS3.ABENDAID.REPORTDB) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(SYS3.ABENDAID.REPORTDB) ACCESS(READ)
TSS PERMIT(appdaudt) DSN(SYS3.ABENDAID.REPORTDB) ACCESS(CONTROL)
TSS PERMIT(appsaudt) DSN(SYS3.ABENDAID.REPORTDB) ACCESS(CONTROL)
TSS PERMIT(syspaudt) DSN(SYS3.ABENDAID.SHARED) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.ABENDAID.SHARED) ACCESS(ALL)
TSS PERMIT(ABEND-AID STCs) DSN(SYS3.ABENDAID.SHARED) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(SYS3.ABENDAID.SHARED) ACCESS(READ)
TSS PERMIT(appdaudt) DSN(SYS3.ABENDAID.SHARED) ACCESS(CONTROL)
TSS PERMIT(appsaudt) DSN(SYS3.ABENDAID.SHARED) ACCESS(CONTROL)

CCI: CCI-000213

Group ID (Vulid): V-17947

Group Title: ZB000020
Rule ID: SV-44086r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDT020
Rule Title: Compuware Abend-AID resources must be properly defined and protected.

Vulnerability Discussion: Compuware Abend-AID 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.

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

- SENSITVE.RPT(ZAID0020)
- TSSCMDS.RPT(#RDT)

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

- PDI(ZAID0020)

Note: The Abend-AID resource class is identified in the Enterprise Common Components (ECC) STC procedure, CWPARM DD statement, member name AAVW00, using the parameter setting EXTERNAL_SECURITY_RESOURCE_CLASS.

Verify that the accesses to resources and/or generic equivalent are properly restricted according to the requirements specified in Compuware Abend-AID Resources table in the z/OS STIG Addendum.

If the following guidance is true, this is not a finding.

___ The TSS resources are owned or DEFPROT is specified for the resource class.

___ The TSS resource access authorizations restrict access to the appropriate personnel.

Fix Text: Ensure 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 prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Use Compuware Abend-AID Resources and Compuware Abend-AID Resources Descriptions tables in the zOS STIG Addendum. These tables list the resources, descriptions, and access and logging requirements. Ensure the guidelines for the resources and/or generic equivalent specified in the z/OS STIG Addendum are followed.

Note: The Compuware Abend-AID resource class is identified in the Viewer Server's STC configuration procedure, CWPARM DD statement, member name AAVW00, using the parameter setting EXTERNAL_SECURITY_RESOURCE_CLASS. In addition, there is a parameter that identifies the prefix for all resources, which is EXTERNAL_SECURITY_PREFIX.

The TSS resources as designated in the above table are owned and/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 following commands are provided as a sample for implementing resource controls:

TSS ADD(dept-acid) resource-class(prefix)
TSS PERMIT(appdaudt) res-class(prefix.SERVER.LOGON.FD.) ACCESS(ALL)
TSS PERMIT(appsaudt) res-class(prefix.SERVER.LOGON.FD.) ACCESS(ALL)
TSS PERMIT(operaudt) res-class(prefix.SERVER.LOGON.FD.) ACCESS(ALL)
TSS PERMIT(syspaudt) res-class(prefix.SERVER.LOGON.FD.) ACCESS(ALL)

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-43176r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDT030
Rule Title: Compuware Abend-AID Started Task name will be properly identified and/or defined to the system ACP.

Vulnerability Discussion: Compuware Abend-AID requires a started task that will 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.

Check Content:
Default Finding Details:
The product's started task(s) is (are) not properly identified and/or defined to the System ACP.

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

- TSSCMDS.RPT(@ACIDS)

Verify that the ACID(s) for the Compuware Abend-AID started task(s) is (are) properly defined. If the following attributes are defined, this is not a finding.

FACILITY(STC, BATCH)
PASSWORD(xxxxxxxx,0)
SOURCE(INTRDR)
NOSUSPEND

Fix Text: The IAO working with the systems programmer will ensure the Compuware Abend-AID Started Task(s) is properly identified and/or 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.

The following commands are provided as a sample for defining Started Task(s):

```
TSS CREATE(BDCAS) TYPE(USER) -
     NAME('STC, Compuware Abend-AID') DEPT(xxxx) -
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
TSS CREATE(TDCAS) TYPE(USER) -
     NAME('STC, Compuware Abend-AID for CICS') DEPT(xxxx) -
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
```

```
TSS CREATE(AAVIEWER) TYPE(USER) -
     NAME('STC, Compuware Abend-AID Viewer') DEPT(xxxx) -
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-43186r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDT032
Rule Title: Compuware Abend-AID Started task will be properly defined to the Started Task Table 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.

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(ZAID0032)

If the Compuware Abend-AID started task(s) is (are) defined in the TSS STC record, this is not a finding.

Fix Text: The IAO working with the systems programmer will ensure the Compuware Abend-AID Started Task(s) is properly identified and/or defined to the System ACP.

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

The following commands are provided as a sample for defining Started Task(s):

```
TSS ADD(STC) PROCNAME(AAVIEWER) ACID(AAVIEWER)
TSS ADD(STC) PROCNAME(BDCAS) ACID(BDCAS)
TSS ADD(STC) PROCNAME(TDCAS) ACID(TDCAS)
```

CCI: CCI-000764

UNCLASSIFIED