

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS Compuware Abend-AID for ACF2 STIG

Version: 6

Release: 5

29 Dec 2020

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-43205r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAID0040
Rule Title: Compuware Abend-AID external security options will 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.

Responsibility: Systems Programmer
IAControls: ECCD-1, ECCD-2

Check Content:

- a) Use TSO option 3.4 to see the name of the Contents Dataset specified in the FDBDPARM DD statement in the Abend Aid started task procedure.
- b) Check the Contents Dataset for the setting of the parameter "External_Security_Enabled".
- c). If the setting of this parameter is "YES", there is NO FINDING.
- d) If the setting of this parameter is "NO", there is a FINDING.

Fix Text: The systems programmer/IAO will ensure that the Compuware Abend-AID parameter is (are) specified. Compuware Abend-AID security interfaces are controlled by parameters coded in the data set specified in the FDBDPARM DD statement of the started task procedures.

Parameter	Value
EXTERNAL_SECURITY_ENABLED	YES

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-43166r1_rule
Severity: CAT II

Rule Version (STIG-ID): ZAIDR000

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.

Responsibility: Information Assurance Officer

IACControls: 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:

- SENSITIVE.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 ACF2 data set rules for the data sets restricts READ access to all authorized users.

___ The ACF2 data set rules for the data sets restricts WRITE and/or greater access to systems programming personnel.

___ The ACF2 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:

\$KEY(S2A)

\$PREFIX(SYS2)

ABENDAID.V.- UID(syspauDt) R(A) W(L) A(L) E(A)

ABENDAID.V.- UID(authorized users/*) R(A) E(A)

SET RULE

COMPILE 'ACF2.MVA.DSNRULES(S2A)' STORE

\$KEY(SYS2A0A)

\$MODE(ABORT)

\$PREFIX(SYS2A)

ABENDAID.V.- UID(syspauDt) R(A) W(L) A(L) E(A)

ABENDAID.V.- UID(authorized users/*) R(A) E(A)

SET RULE

COMPILE 'ACF2.MVA.DSNRULES(SYS2A0A)' STORE

\$KEY(SYS3A0A)

\$PREFIX(SYS3A)

ABENDAID.V.- UID(syspauDt) R(A) W(L) A(L) E(A)

ABENDAID.V.- UID(authorized users/*) R(A) E(A)

SET RULE

COMPILE 'ACF2.MVA.DSNRULES(SYS3A0A)' STORE

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067

Group Title: ZB000001

Rule ID: SV-43169r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZAIDR001

Rule Title: Compuware Abend-AID STC data sets must 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.

Responsibility: Information Assurance Officer

IAControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

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

- SENSITIVE.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 ACF2 data set rules for the data sets restricts READ access to auditors.

___ The ACF2 data set rules for the data sets restricts WRITE and/or greater access to systems programming personnel.

___ The ACF2 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:

```
$KEY(SYS3)
ABENDAID.- UID(<syspau>) R(A) W(A) A(A) E(A)
ABENDAID.- UID(<tstcaudt>) R(A) W(A) A(A) E(A)
ABENDAID.- UID(ABENDAID STCs) R(A) W(A) A(A) E(A)
ABENDAID.- UID(<audtaudt>) R(A) E(A)
```

CCI: CCI-001499

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-75839r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZAIDR002
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.

Responsibility: Information Assurance Officer
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(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 ACF2 data set rules for the listed data sets restricts READ access to auditors.

___ The ACF2 data set rules for the listed data sets restricts WRITE and/or greater access to systems programming personnel.

___ The ACF2 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 ACF2 data set rules for the listed data sets restricts WRITE access to Application Development Programmers and Application Production Support Team members.

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:

```
$KEY(SYS3)
ABENDAID.- UID(<syspau>) R(A) W(A) A(A) E(A)
ABENDAID.- UID(<tstcaudt>) R(A) W(A) A(A) E(A)
ABENDAID.- UID(ABENDAID STCs) R(A) W(A) A(A) E(A)
ABENDAID.- UID(<audtaudt>) R(A) E(A)
```

CCI: CCI-000213

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-44085r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZAIDR020

Rule Title: Compuware Abend-AID resources will 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.

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

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

SENSITIVE.RPT(ZAID0020)
- ACF2CMDS.RPT(RESOURCE) Alternate report

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 the Compuware Abend-AID Resources table in the z/OS STIG Addendum.

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

___ The ACF2 resources are defined with a default access of PREVENT.

___ The ACF2 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 the Compuware Abend-AID Resources and Compuware Abend-AID Resources Descriptions tables in the z/OS STIG Addendum. These tables list the resources, access requirements, and logging requirement for Compuware Abend-AID. 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 ACF2 resources as designated in the above table are defined with a default access of PREVENT.

The ACF2 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:

```
$KEY(prefix) TYPE(resource-type)
SERVER.LOGON.FD.- UID(appdaudt) ALLOW
SERVER.LOGON.FD.- UID(appsaudt) ALLOW
SERVER.LOGON.FD.- UID(operaudt) ALLOW
SERVER.LOGON.FD.- UID(syspauat) ALLOW
- UID(*) PREVENT
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-43175r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZAIDR030

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.

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

Check Content:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

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

STC

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):

```
au AAVIEWER name('STC, Compuware Abend-AID Viewer') owner(stc) dfltgrp(stc)
nopass
```

```
    data('Abend-AID Viewer')
```

```
au BDCAS name('STC, Compuware Abend-AID') owner(stc) dfltgrp(stc) nopass
    data('Abend-AID')
```

```
au TDCAS name('STC, Compuware Abend-AID for CICS') owner(stc) dfltgrp(stc)
nopass
```

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):

SET LID

insert AAVIEWER stc name('STC, Compuware Abend-AID Viewer')

insert BDCAS stc name('STC, Compuware Abend-AID')

insert TDCAS stc name('STC, Compuware Abend-AID for CICS')
data('Abend-AID')

CCI: CCI-000764

UNCLASSIFIED