

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS Compuware Abend-AID for RACF STIG

Version: 6

Release: 7

30 June 2023

XSL Release 5/15/2012 Sort by: STIGID
Description:

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
 IACcontrols: 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:

a) Consult with your systems programmer to identify the names of the Compuware Abend-Aid product installation datasets (they may likely be called or begin with SYS2.ABENDAID, SYS2A.ABENDAID, or SYS3A.ABENDAID).

b) Ensure the following data set controls are in effect for the Compuware Abend-Aid installation data sets:

- READ access to the Compuware Abend-Aid installation data sets is restricted to authorized users.

- UPDATE or higher access to the Compuware Abend-Aid installation data sets is restricted to systems programming personnel.

- UACC (None) and NOWARNING are specified for the Compuware Abend-Aid installation data sets.

- The RACF data set rules for the Compuware Abend-Aid data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) are logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.

2. Tab down to Data Set row, type LV next to the dataset profile for the Compuware Abend-Aid data sets.

3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.

4. Review the Standard Access List and Conditional Access List on the dataset profile General Information Screen. and verify that access is restricted as specified in b. above.

5. Verify the 'Audit Successes' column on the dataset profile General Information screen . Underneath it should be found 'Successes Write' which means that all successful WRITE access is logged as specified in b. above.

6. Verify the 'Audit Failures' column on the dataset profile General Information screen . Underneath it should be found 'Failures Write' which means that all failed WRITE access is logged as specified in b. above.

7. Repeat steps 1-6 above for any other Compuware Abend-Aid dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the Compuware Abend-Aid installation data sets are restricted to systems programming personnel, there is NO FINDING.

e) If UPDATE and ALLOCATE (ALTER) access to the Compuware Abend-Aid installation sets is not restricted to systems programming personnel there is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING.

g) If UACC is not None or Warning is not No, there is a FINDING.

h) If all accesses of UPDATE or higher are logged there is NO FINDING.

i) If all accesses of UPDATE or higher are not logged, there is a FINDING.

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:

```
AD 'sys2.abendaaid.v**' UACC(NONE) OWNER(SYS2) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys2a.abendaaid.v**' UACC(NONE) OWNER(SYS2A) AUDIT(SUCCESS(UPDATE)
```

```

FAILURES (READ))
AD 'sys3a.abendaaid.v**' UACC(NONE) OWNER(SYS3A) AUDIT(SUCCESS(UPDATE)
FAILURES (READ))

```

```

PE 'sys2.abendaaid.v**' ID(syspau dt) ACC(A)
PE 'sys2.abendaaid.v**' ID(authorized users/*) ACC(R)
PE 'sys2a.abendaaid.v**' ID(syspau dt) ACC(A)
PE 'sys2a.abendaaid.v**' ID(authorized users/*) ACC(R)
PE 'sys3a.abendaaid.v**' ID(syspau dt) ACC(A)
PE 'sys3a.abendaaid.v**' ID(authorized users/*) ACC(R)

```

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

Check Content:

- a) Consult with your systems programmer to identify the names of the Compuware Abend-Aid product STC datasets (they may likely be called or begin with SYS3.ABENDAID).
- b) Ensure the following data set controls are in effect for the Compuware Abend-Aid STC data sets:
 - READ access to the Compuware Abend-Aid product STC data sets can be given to auditors.
 - UPDATE or higher access to the Compuware Abend-Aid product STC data sets is restricted to systems programming personnel and/or Abend Aid STCs and/or batch users.

- UACC (None) and NOWARNING are specified for the Compuware Abend-Aid product
STC data sets.

- The RACF data set rules for the Compuware Abend-Aid STC data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.
2. Tab down to Data Set row, type LV next to the dataset profile for the Compuware Abend-Aid STC data sets.
3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
4. Review the Standard Access List and Conditional Access List areas on the dataset profile General Information Screen and verify that access is restricted as specified in b) above.
5. Verify the 'Audit Successes' and 'Audit Failures' column on the dataset profile General Information screen . They should specify 'Successes Write' and 'Failures Write' respectively.
6. Repeat steps 1-5 above for any other Compuware Abend-Aid STC dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the Compuware Abend-Aid STC data sets are specified as in b) above, there is NO FINDING.

e) If UPDATE and ALLOCATE (ALTER) access to the Compuware Abend-Aid sets is not restricted as in b) above there is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING

g) If UACC is not None or Warning is not No, this is a FINDING..

h) If logging is as specified in b. above there is NO FINDING.

i) If logging is not as specified in b. above there is a FINDING.

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:

```
AD 'sys3.abendaaid.**' UACC(NONE) OWNER(SYS3) AUDIT(FAILURES(READ))
```

```
PE 'sys3.abendaaid.**' ID(syspautd) ACC(A)
PE 'sys3.abendaaid.**' ID(ABENDAID STCs) ACC(A)
PE 'sys3.abendaaid.**' ID(audtautd) ACC(R)
```

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:

a) 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

b) Ensure the following data set controls are in effect for the Compuware Abend-Aid User data sets:

- READ access to the Compuware Abend-Aid User datasets can be given to auditors.

- UPDATE or higher access to the Compuware Abend-Aid User datasets is restricted to systems programming personnel and/or Abend Aid STCs and/or batch users

- CONTROL access to the Compuware Abend-Aid User datasets is restricted to Application Development Programmers and Application Production Support Team members.

- UACC (None) and NOWARNING are specified for the Compuware Abend-Aid User data sets.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.

2. Tab down to Data Set row, type LV next to the dataset profile for the Compuware Abend-Aid User data sets.

3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.

4. Review the Standard Access List and Conditional Access List areas on the dataset profile

General Information Screen and verify that access is restricted as specified in b) above.

5. Verify the 'Audit Successes' and 'Audit Failures' column on the dataset

profile General Information screen . They should specify 'Successes Write' and 'Failures Read' respectively.

6. Repeat steps 1-5 above for any other Compuware Abend-Aid User dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the Compuware Abend-Aid User data sets are specified as in b) above, there is NO FINDING.

e) If UPDATE and ALLOCATE (e.g. ALTER) access to the Compuware Abend-Aid User datasets is not restricted as in b) above there is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING

g) If UACC is not None or Warning is not No, this is a FINDING..

Fix Text: Ensure that WRITE and/or greater access to Compuware Abend-AID User data sets listed is limited to System Programmers and/or 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:

```
AD 'sys3.abendaid.shared.**' UACC(NONE) OWNER(SYS3) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys3.abendaid.reportdb.**' UACC(NONE) OWNER(SYS3)
AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
```

```
PE 'sys3.abendaid.reportdb.**' ID(syspau dt) ACC(A)
PE 'sys3.abendaid.reportdb.**' ID(tstcau dt) ACC(A)
PE 'sys3.abendaid.reportdb.**' ID(ABEND-AID STCs) ACC(A)
PE 'sys3.abendaid.reportdb.**' ID(audtau dt) ACC(R)
PE 'sys3.abendaid.reportdb.**' ID(appdau dt) ACC(CONTROL)
PE 'sys3.abendaid.reportdb.**' ID(appsau dt) ACC(CONTROL)
PE 'sys3.abendaid.shared.**' ID(syspau dt) ACC(A)
PE 'sys3.abendaid.shared.**' ID(tstcau dt) ACC(A)
PE 'sys3.abendaid.shared.**' ID(ABEND-AID STCs) ACC(A)
PE 'sys3.abendaid.shared.**' ID(audtau dt) ACC(R)
PE 'sys3.abendaid.shared.**' ID(appdau dt) ACC(CONTROL)
PE 'sys3.abendaid.shared.**' ID(appsau dt) ACC(CONTROL)
```

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:

a) From the Administrator main menu, select 3;4 (Security Server Reports, General Resource Profiles) and press ENTER.

b) Tab down to CLASS and enter the Abend-Aid resource class name and press ENTER.

(The Abend-Aid resource class name can be found in the Abend Aid STC JCL. It is the value specified for the EXTERNAL_SECURITY_RESOURCE_CLASS parameter in the configuration file defined on the FDBPARM DD statement).

c) Check the profiles that are displayed on the General Resource Profile. Summary screen. For any profiles on the display that are found in the Compuware

Abend Aid Resources table in the z/OS STIG addendum:

1. Verify that they are defined with a UACC=NONE.
2. Type LR in the CMD column of each resource name and check that:
 - warning is set to NO
 - the list of users and conditional access users only include users that belong to the groups specified in the COMPUWARE Abend-Aid resources table**.
 - the access level for each user is ALTER or less.

** (To check if a user belongs to one of the groups in the COMPUWARE Abend-Aid resources table:

- Select Option 3;2 from the Administrator Main Menu (Security Server Reports, Group Profiles).

- On the Group Reports Menu, enter 1 at the Command line (for Group Profile Summary).
- Then tab down to Group and enter the Group Name from the resources table and hit enter.
- On the next panel enter LV next to the group name and hit enter.
- The General Information Screen that comes up will have the list of Connected Users).

d) If

- WARNING is not set to NO or
- UACC is not NONE or
- any users are granted access who are not in the Compuware Abend Aid Resources table or
- access is greater than ALTER for any Abend Aid Resource there is a FINDING.

e) If none of the conditions in d) above are true, then there is NO FINDING.

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 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 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 data set, FDBDPARM DD statement, 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 RACF resources as designated in the above table are defined with a default access of NONE.

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

The RACF resource rules for the resources designated in the above table specify UACC(NONE) and NOWARNING.

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

```
RDEFINE resource-class prefix.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
PERMIT prefix.SERVER.LOGON.FD.** CLASS(res-class) ACCESS(ALTER)
ID(appdautd)
PERMIT prefix.SERVER.LOGON.FD.** CLASS(res-class) ACCESS(ALTER)
ID(appsautd)
PERMIT prefix.SERVER.LOGON.FD.** CLASS(res-class) ACCESS(ALTER)
ID(operautd)
PERMIT prefix.SERVER.LOGON.FD.** CLASS(res-class) ACCESS(ALTER)
ID(syspautd)
```

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:

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.
- b) Type 1 for General Resource Profile Summary and Tab down to CLASS, type STARTED for class name and hit Enter.
- c) Find the Abend Aid General Resource profile and enter LR next to it and hit Enter. If not found go to step k. below.
- d) Find the userid associated with the Abend Aid started task under the STDATA segment information of the Abend Aid general resource profile.
- e) Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press Enter.
- f) Enter 2 (for User Attributes) and tab down to User ID and enter the User ID found in Step d) above and hit Enter.
- g) If the last column on the screen (PROT) is set to "PT", the Userid has the PROTECTED attribute set. If the last column is blank, the Userid does not have the PROTECTED attribute set.
- h) If PROTECTED = Yes, there is no FINDING.
- i) If PROTECTED = No, there is a FINDING.
- j) End Check.
- k) If Abend Aid is NOT found as a General Resource profile under the STARTED class in c. above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:
 - 1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press ENTER
 - 2. Look for STARTED in the Source column and the Abend Aid started task procname in the Procname column.
 - 3. If the Abend Aid started procedure does not have an R in the M column there is

NO FINDING (an R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)).

4. If there is an R in the M column, there is 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.

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
    data('Abend-AID')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
 Group Title: ZB000032
 Rule ID: SV-43185r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZAIDR032
 Rule Title: Compuware Abend-AID Started task will be properly defined to the STARTED resource class for RACF.

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.

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

Check Content:

a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.

b) Type 1 for General Resource Profile Summary and tab down to CLASS and enter 'STARTED' for class name.

c) Find the Abend Aid started task procname..

d). If found, there is NO FINDING.

e) If not found, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:

1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press Enter.

2. Look for STARTED in the Source column and the ABEND AID started task proc name in the Procname column

3. If found, there is NO FINDING.

4. If it is not found, there is 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 userid must be assigned for the Compuware Abend-AID started task(s) thru a corresponding STARTED class entry.

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

```
rdef started AAVIEWER.** uacc(none) owner(admin) audit(all(read))
      stdata(user(AAVIEWER) group(stc))
rdef started BDCAS.** uacc(none) owner(admin) audit(all(read))
      stdata(user(BDCAS) group(stc))
rdef started TDCAS.** uacc(none) owner(admin) audit(all(read))
      stdata(user(TDCAS) group(stc))
```

setr racl(started) ref

CCI: CCI-000764

UNCLASSIFIED