

UNCLASSIFIED



z/OS Websphere Application Server for RACF STIG

Version: 6

Release: 1

6 Jun 2020

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

---

Group ID (Vulid): V-3897

Group Title: ZWAS0010

Rule ID: SV-3897r3\_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0010](#)

Rule Title: MVS data sets for the WebSphere Application Server are not protected in accordance with the proper security requirements.

Vulnerability Discussion: MVS data sets provide the configuration, operational, and executable properties of the WebSphere Application Server (WAS) environment. Failure to properly protect these data sets may lead to unauthorized access. This exposure could compromise the integrity and availability of system services, applications, and customer data.

Responsibility: Information Assurance Officer IAControls:

DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Generate online data set reports using Administrator for the listed data set resources.

1. Option 3 Security Server Reports from the main menu
2. Option 3 Data Set Profile
3. Enter IMW\* in the Data Set: field.
4. Enter command 4 Access Lists to review the high level qualifier5. Issue the S Access List command to review access levels as required.

b) Ensure the following data set controls are in effect for WAS:

1. UPDATE and ALTER access to HTTP product data sets (i.e., hlq.IMW.AIMW\*\* and hlq.IMW.SIMW\*\*) is restricted to systems programming personnel.

NOTE: If the HTTP server is not used with WAS, this check can be ignored.

2. UPDATE and ALTER access to WAS product data sets and associated product data sets is restricted to systems programming personnel.

hlq.EJS.V3500108.\*\* (WebSphere 3.5)

hlq.WAS.V401.\*\* (WebSphere 4.0.1)

hlq.OE.\*\* (Java) hlq.JAVA\*\*

(Java) hlq.DB2.V710107.\*\*.

(DB2) hlq.GLD.\*\* (LDAP)

hlq.LE.\*\* (Language Environment)

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: The IAO will ensure that WebSphere server data sets restrict UPDATE and/or ALTER access to systems programming personnel.

Ensure the following data set controls are in effect for WAS:

1) UPDATE and ALTER access to HTTP product data sets (i.e., SYS1.IMW.AIMW\*\* and SYS1.IMW.SIMW\*\*) are restricted to systems programming personnel.

NOTE: If the HTTP server is not used with WAS, this check can be ignored.

2) UPDATE and ALTER access to WAS product data sets and associated product data sets are restricted to systems programming personnel.

SYS\*.EJS.V3500108.\*\* (WebSphere 3.5)

SYS\*.WAS.V401.\*\* (WebSphere 4.0.1)

SYS\*.OE.\*\* (Java)

SYS\*.JAVA\*\* (Java)

SYS\*.DB2.V710107.\*\* (DB2)

SYS\*.GLD.\*\* (LDAP)

SYS1.LE.\*\* (Language Environment)

CCI: CCI-000213

---

Group ID (Vulid): V-3898

Group Title: ZWAS0020

Rule ID: SV-3898r3\_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0020](#)

Rule Title: HFS objects for the WebSphere Application Server are not protected in accordance with the proper security requirements.

Vulnerability Discussion: HFS directories and files provide the configuration, operational, and executable properties of the WebSphere Application Server (WAS) environment. Many of these objects are responsible for the security implementation of WAS. Failure to properly protect these directories and files may lead to unauthorized access. This exposure could potentially compromise the integrity and availability of system services, applications, and customer data.

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

Check Content:

a) Use Administrator option 14 Unix File Manager to determine the owner, Group, and permissions of the file system paths in the tables below. Use the XA command to expand the audit fields for verification.

Refer to the following item gathered from the IBM HTTP Server Worksheet in the Preliminary Information Worksheets:

1. DOC(IHSACCTS)

b) The following notes apply to the requirements specified in the subsequent tables:

- \* If an owner field indicates UID(0) user, any system ID with a UID(0) specification is acceptable.
- \* Where an owner field indicates webserv1, the ID of the web server is intended.\* Where a group field indicates webadmg1, the ID of a local web server administration group is intended. IMWEB is not a valid local group.
- \* The site is free to set the permission and audit bit settings to be more restrictive than the documented values.

Ensure the HFS permission bits, user audit bits, owner, and group for each directory and file match the specified settings listed in the following tables:

**IHS VENDOR SERVER SOFTWARE HFS OBJECT SECURITY SETTINGS**  
**DIRECTORY or FILE PERMISSION USER AUDIT OWNER GROUP**  
**BITS BITS**

/usr/lpp/internet 755 fff UID(0) user IMWEB

/usr/lpp/internet/bin 755 fff UID(0) user IMWEB

/usr/lpp/internet/sbin 750 fff UID(0) user IMWEB

**IHS LOCAL SERVER STANDARD HFS OBJECT SECURITY SETTINGS**  
**DIRECTORY or FILE PERMISSION USER AUDIT OWNER GROUP**

**BITS BITS**

```
/websrv1_root/ 555 fff websrv1 webadmg1  
/websrv1_root/Admin 550 fff websrv1 webadmg1  
/websrv1_root/admin-bin 550 fff websrv1 webadmg1  
/websrv1_root/cgi-bin 551 fff websrv1 webadmg1  
/websrv1_root/cgi-bin 550 fff websrv1 webadmg1  
/websrv1_root/pub 555 fff websrv1 webadmg1
```

**IHS LOCAL SERVER CONFIGURATION HFS OBJECT SECURITY SETTINGS  
DIRECTORY or FILE PERMISSION USER AUDIT OWNER GROUP  
BITS BITS**

```
/etc/websrv1/httpd.conf 460 faf websrv1 webadmg1  
/etc/websrv1/httpd.envvars 564 faf websrv1 webadmg1  
/etc/websrv1/mvsds.conf 460 faf websrv1 webadmg1
```

**IHS LOCAL SERVER LOG HFS OBJECT SECURITY SETTINGS  
DIRECTORY or FILE PERMISSION USER AUDIT OWNER GROUP  
BITS BITS**

```
/websrv1_root/logs 750 fff websrv1 webadmg1  
/websrv1_root/logs/httpd-log 750 fff websrv1 webadmg1  
/websrv1_root/logs/httpd-errors 750 fff websrv1 webadmg1 /websrv1_root/logs/cgi-  
error 750 fff websrv1 webadmg1
```

NOTE: The HFS permission bits, user audit bits, owner, and group settings specified for the WAS configuration and property files in Section 17.2.3.6 of the Z/OS STIG V4R1 is incorrect. The general guidance that was used in this section was taken from the Web Server STIG which was determined to be incorrect. Currently the STIG requires the permissions on these files to be 640, where the group is the SA or web manager account that controls the web service. However the group permission only allows READ access making it impossible to update files unless using a UID(0) account. There appears to be a conflict with this requirement.

Proposed Z/OS STIG updates include changing permissions from 640 to 460. The owner will be the web server user account and the group will be the web server administrator group. The Web Server STIG is looking into using these same settings. Verification of these proposed changes needs to be performed and the Z/OS STIG updated. Until this occurs, compliance of the WAS configuration and property files cannot be reviewed. An entry for was.conf file settings needs to be added to the STIG as well. Settings for the WebSphere properties and bin directories may be desirable.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7 rwx(least restrictive)  
6 rw3  
-wx  
2 -w-  
5 r-x  
4 r--
```

1 --x

0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts a log

for failed and successful access

- no auditing

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: Review the UNIX permission bits, user audit bits, and ownership settings on the HFS directories and files for the products required to support the WAS environment.

Ensure the HFS permission bits, user audit bits, owner, and group for each directory and file match the specified settings listed in the HFS Permissions Bits table located in the zOS STIG Addendum.

CCI: CCI-000213

CCI: CCI-002234

---

Group ID (Vulid): V-3899

Group Title: ZWAS0030

Rule ID: SV-7265r3\_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0030](#)

Rule Title: The CBIND Resource Class for the WebSphere Application Server is not configured in accordance with security requirements.

Vulnerability Discussion: SAF resources provide the ability to control access to functions and services of the WebSphere Application Server (WAS) environment. Many of these resources provide operational and administrative support for WAS. Failure to properly protect these resources may lead to unauthorized access. This exposure could compromise the integrity and availability of application services and customer data.

Responsibility: Information Assurance Officer IAControls:

N/A

Check Content:

a) Verify the following items using Administrator:

1. Option 3 Security Server Reports from the main menu.
2. Option 4 General Resource Profile
3. Under the Standard Masking Fields enter CBIND in the Class: field4. At the resulting report enter LV in the command area to verify access levels for item 3 below.

b) Ensure the following items are in effect for CBIND resource protection:

1. The CBIND resource class is active.
2. The CB.BIND.server\_name and CB.server\_name resources is defined to the CBIND resource class with a UACC(NONE).
3. Access to the CB.BIND.server\_name and CB.server\_name resources is restricted to WAS server (STC) userids and systems management userids (e.g., WebSphere administrator ID).

c) If all items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: There are two profiles to create when using the CBIND class. They are the CB.BIND.server\_name profile, which controls whether a local or remote client can access servers. The CB.BIND is mandatory for the first two qualifiers for the profile; the third qualifier is the server name. Also, there is the CB.server\_name profile that controls whether a client can use components in a server; again these definitions are mandatory.

Ensure the following items are in effect for CBIND resource protection:

- 1) The CBIND resource class is active.
- 2) The CB.BIND.server\_name resource is defined to the CBIND resource class with a UACC(NONE).
- 3) Access to the CB.BIND.server\_name resource is restricted to WAS server (STC) userids and systems management userids (e.g., WebSphere administrator ID).

The following command provide sample definitions and permissions for this CBIND resource:

```
SETR CLASSACT(CBIND)  
SETR GENERIC(CBIND)  
SETR RACL(CBIND)
```

```
RDEFINE CBIND cb.bind.<servername> UACC(none) owner(admin) audit(all(read)) data('IAW SRR PDI  
ZWAS0030')
```

```
Permit cb.bind.<servername> CLASS(CBIND) ID(<wscfg1>) ACCESS(CONTROL)
```

Note: "wscfg1" is a RACF group that contains the Websphere Application Server STCs and maintenance userids.

CCI: CCI-000213



---

Group ID (Vulid): V-3900

Group Title: ZWAS0040

Rule ID: SV-3900r4\_rule

Severity: CAT I

Rule Version (STIG-ID): [ZWAS0040](#)

Rule Title: Vendor-supplied user accounts for the WebSphere Application Server must be defined to the ACP.

Vulnerability Discussion: Vendor-supplied user accounts are defined to the ACP with factory-set passwords during the installation of the WebSphere Application Server (WAS). These user accounts are common to all WAS environments and have access to restricted resources and functions. Failure to delete vendor-supplied user accounts from the ACP may lead to unauthorized access. This exposure could compromise the integrity and availability of system services, applications, and customer data.

Responsibility: Information Assurance Officer IAControls:

N/A

Check Content:

a) Create an online user report using Administrator

1. Option 3 Security Server Reports

2. Option 1 User Profile

3. Enter CBADMIN on the User ID: masking field

4. Enter command option 1 to generate the report

5. Use the LV command to review the PWD Last Changed: information.

b) If the CBADMIN user account is not defined to RACF, there is NO FINDING.

c) If the CBADMIN user account is defined to RACF and the password has NOT been changed from the vendor default of CBADMIN, this is a FINDING with a severity code of CAT I.

d) If the CBADMIN user account is defined to RACF and the password has been changed from the vendor default of CBADMIN, this is a FINDING with a severity code of CAT II.

Fix Text: The IAO will ensure that the CBADMIN user account is removed or not defined to the ACP.

CCI: CCI-001762

---

Group ID (Vulid): V-3901 Group

Title: ZWAS0050

Rule ID: SV-3901r3\_rule

Severity: CAT II

Rule Version (STIG-ID): [ZWAS0050](#)

Rule Title: The WebSphere Application Server plug-in is not specified in accordance with the proper security requirements.

Vulnerability Discussion: Requests processed by the WebSphere Application Server (WAS) are dependent on directives configured in the HTTP server httpd.conf file. These directives specify critical files containing the WAS plug-in and WAS configuration. These files provide the operational and security characteristics of WAS. Failure to properly configure WAS-related directives could lead to undesirable operations and degraded security. This exposure may compromise the availability and integrity of applications and customer data.

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

Check Content:

a) Refer to the following item gathered from the IBM HTTP Server Worksheet in the Preliminary Information Worksheets:

1. DOC(IHSPROCS)

b) Review the HTTP server JCL procedure to determine the httpd.conf file to review.

c) Ensure that all WAS-related directives are configured using the ServerInit, Service, and ServerTerm statements as outlined below.

The following path entries were added to the /etc/httpd.conf file for WebSphere 3.5:

```
ServerInit _/usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit
/usr/lpp/WebSphere/etc/WebSphere/AppServer/properties/was.conf
Service _/webapp/examples/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.jhtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.shtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/servlet/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.jsp /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
ServerTerm _/usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit
```

The following path entries are added to the /etc/httpd.conf file for WebSphere 4.0.1:

```
ServerInit - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:init_exit
Service - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:service_exit
ServerTerm - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:term_exit
```

NOTE:\_The /etc/WebSphere clause for ServerInit matches the directory name above where the site customization was.conf file was established.

. Specific items to review include proper path, was.conf, and plug-in settings.

- d) If all WAS-related directives are configured properly, there is NO FINDING.
- e) If any WAS-related directive is not configured properly, this is a FINDING.

Fix Text: The IAO will ensure that the WebSphere Application Server directives in the httpd.conf file are configured as outlined below.

Ensure that all WAS-related directives are configured using the ServerInit, Service, and ServerTerm statements as outlined below.

The following path entries were added to the /etc/httpd.conf file for WebSphere 3.5:

```
ServerInit /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit
/usr/lpp/WebSphere/etc/WebSphere/AppSe
Service /webapp/examples/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /*.jhtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /*.shtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /servlet/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service /*.jsp /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
ServerTerm /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit
```

The following path entries are added to the /etc/httpd.conf file for WebSphere 4.0.1:

```
ServerInit -/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:init_exit
Service - /usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:service_exit
ServerTerm - /usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:term_exit
```

NOTE: The /etc/WebSphere clause for ServerInit matches the directory name above where the site customization was.conf file was established. Specific items to review include proper path, was.conf, and plug-in settings.

CCI: CCI-000068

CCI: CCI-000382

CCI: CCI-001762

---

UNCLASSIFIED