Product Support Notice

PSN #	PSN020297u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 11-Jun-17. This is Issue #01, published date: 11-Jun-17.	Severity/risk level	High	Urgency	Immediately

Name of problem Remote code execution possible.

Products affected

Avaya Aura® Application Enablement (AE) Services 6.3.x - 7.1 (All offers)

Problem description

An AE Services vulnerability allows remote code execution if specially crafted messages are employed.

Avaya thanks Kyle Gaertner of Digital Defense, Inc for reporting this issue.

Resolution

Install the AE Services Security Hotfix.

AE Services 7.1.0.0.0: AES-7-1-0-0-0_Hotfix_Patch_Issue16349.bin
AE Services 7.0.1.0.4: AES-7-0-1-0-4_Hotfix_Patch_Issue16349.bin
AE Services 6.3.3.7: AES-6-3-3-7_Hotfix_Patch_Issue16349.bin

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Backup AE Services server data before applying the Security Hotfix:

1. Log into the AE Services Management Console using a browser.
2. From the main menu, select **Maintenance > Server Data > Backup**.
   AE Services backs up the database, and displays `The backup file can be downloaded from Here` on the **Database Backup** screen,
3. Click the "**Here**" link.
   A file download dialog box is displayed, from where you can open or save the backup file *serverName_SoftwareVersion*_aesvcsdb*ddmmyyyy*.tar.gz. Where, ddmmyyyy is the date stamp).
4. Click **Save**, and download the backup file to a location from where you can gain access in the unlikely event a restore is required. For example, save the file to your local computer or another computer used for storing backups.

Download

To download the AE Services security Hotfix:

A. Download from the Ayava support site:
   1. Go to Avaya Support (http://support.avaya.com).
   2. Click Support by Products > **Downloads**:
      i. In Enter Product Name type *"Avaya Aura Application Enablement Services"*
      ii. In Choose Release select the appropriate release from the drop-down menu.
      iii. In the list of Downloads locate and select the appropriate Security Hotfix download (paging might be necessary to find the entry).

B. To download from PLDS
   1. Go to the link- https://plds.avaya.com.
   2. Enter your login ID and password. You may have to search for and enter your company name and/or accept the one time EULA to gain access to software download.
   3. Select **View Downloads**.
   4. In the **Search by Download** tab enter the correct PLDS ID (see the tables below) in the **Download pub ID** search

field and select **Search Downloads**.

5. Select the **Download** link to begin the download

AE Services 7.1.0.0.0:

PLDS ID	AES00000570
File Name	AES-7-1-0-0-0_Hotfix_Patch_Issue16349.bin
MD5 Sum	1f2aae6bbcf1f4884e665b7a5f8e0364

AE Services 7.0.1.0.4:

PLDS ID	AES00000569
File Name	AES-7-0-1-0-4_Hotfix_Patch_Issue16349.bin
MD5 Sum	4a9a0c9e5fa46a51bfe5bc370d0c6093

AE Services 6.3.3.7:

PLDS ID	AES00000568
File Name	AES-6-3-3-7_Hotfix_Patch_Issue16349.bin
MD5 Sum	b717009b6385c29e73f3d12794241a1b

Before you start with the installation of the patch, check the md5 checksum of the file.

To get the checksum, run the following command from the command line:

md5sum <filename>.bin

Note: If the MD5 checksum does not match the stated value, do not proceed with installation. Download the patch again and verify the MD5 checksum matches.

Patch install instructions	Service-interrupting?
Steps to install the security Hotfix:	Yes

1. Login to the AE Services server using the local Linux console, the services port or SSH.
2. Secure copy (SCP) the AES-<**version**>_Hotfix_Patch_Issue16349.bin patch to the /tmp directory on the AE Services server.
3. As the root user, execute the following from the command line:
   cd /tmp
   chmod 750 AES-<**version**>_Hotfix_Patch_Issue16349.bin
   ./AES-<**version**>_Hotfix_Patch_Issue16349.bin
4. Follow the on-screen instructions carefully.
   You should see output similar to the following. This example is for AE Services 7.1.0.0.0:

```
[root@server tmp]# ./AES-7-1-0-0-0_Hotfix_Patch_Issue16349.bin
Installing hotfix patch on AE Services 7.1.0.0.0
Installing this hotfix patch will restart the tomcat service
Do you want to proceed with this installation? Enter [y/n] :y
Updating aesvcs.war for AE Services 7.1.0.0.0
Stopping Tomcat service
Backing up old aesvcs.war as /tmp/aesvcs.war.bk
Copying new aesvcs.war
Copying aesvcs.war file successful
Starting tomcat service
Tomcat is running
Waiting up to 30 seconds for aesvcs servlet deployment
Waiting up to 30 seconds
Waiting up to 29 seconds
Waiting up to 28 seconds
Waiting up to 27 seconds
Deployment successful
Removing temporary directory
```

Note: **<version>** refers to the AE Services version number in the name of the hotfix patch that is being installed.

Verification

1. Login to the AE Services server using the local Linux console, the services port or SSH.
2. As the root user execute: md5sum /usr/share/tomcat5/webapps/aesvcs.war
3. Verify the calculated md5sum matches the md5sum for the appropriate AE Services version:
   - AE Services 6.3.3 aesvcs.war md5sum = d1189e464fa236ba7e76f57e2406d123
   - AE Services 7.0.1 aesvcs.war md5sum = daa3fbe30af8ff8739706787f867b384
   - AE Services 7.1.0 aesvcs.war md5sum = 8875d2dd766159146804e05d530d43a1
4. Execute ls –l /usr/share/tomcat5/webapps
5. Verify the timestamp for the aesvcs.war file and deployed aesvcs directory has the same date.
6. Using a web browser, log into the AE Services Management Console to verify the Management Console is accessible.

Failure

Contact Technical Support.

Patch uninstall instructions

The Security Hotfix cannot be uninstalled.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Failure to apply the Security Hotfix has the potential to result in a security breach.

Avaya Security Vulnerability Classification

High

Mitigation

Install the AE Services Security Hotfix.

Reference ASA-2017-088.

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.