AVAYA

Product Support Notice

PSN #	PSN003161u				
Original publication date: 14-Feb-11. This is Issue # 01, published date: 14-Feb-11.		Severity/risk level	Medium	Urgency	When convenient
Name of problem	Application Enablement Services (AES): Release 4.2.4 Super Patch 1				

Products affected

Application Enablement Services (AES): Release 4.2.4 Bundled Server / Software Only Offer

Problem description

What is fixed in this Patch?

This patch contains the following update to OAM:

Issue AES00809935: ASA-2010-339: AES Authorization Bypass Vulnerability
A flaw was discovered in the AES OAM web interface which could allow non-privileged AES OAM users to perform some operations that are intended to be restricted to privileged OAM users only allowing for an authorization bypass and privilege escalation. This issue is now resolved.

Resolution

Install Super Patch 1 for AES 4.2.4.

Workaround or alternative remediation

n/a

Remarks

1. **Which AE Services rpm/s are updated by AE Services 4.2.4 Super Patch 1?**
   mvap-platform-4.2.4.506-1.noarch.rpm
2. **Are there new features or enhancements included in AE Services 4.2.4 Super Patch 1?**
   AE Services 4.2.4 Super Patch 1 does not include new features or enhancements.
3. **What must application suppliers do to be compatible with AE Services 4.2.4 Super Patch 1? (Recompile, re-link and so on.)**
   Super Patch 1 is fully compatible with AE Services 4.x.x Clients and SDKs.
4. **Is applying this Super Patch service affecting?**
   The Application Enablement Server will be out of service for 20 to 30 minutes while the Super Patch is being applied.
5. **With which Application Enablement Services release(s) is Super Patch 1 compatible?**
   AE Services 4.2.4.
6. **Is AE Services 4.2.4 Super Patch 1 cumulative?**
   Does not apply.
7. **Is AE Services 4.2.4 Super Patch 1 compatible with Application Enablement Services 3.x, 4.0, 4.01, 4.1, 4.2.1, 4.2.2, and 4.2.3 servers?**
   No. AE Services 3.x, 4.0, 4.1, 4.2.1, 4.2.2, and 4.2.3 must first be upgraded to AE Services 4.2.4, only then can Super Patch 1 be applied.
8. **What are the CM requirements for Application Enablement Services 4.2.3 Super Patch 2?**
   AE Services 4.2.3 Super Patch 2 supports CM 3.x.x or higher.

Note:

- Certain functionality on AES 4.2.3 requires CM versions later than CM 3.x.
- Support for CM 3.x is limited to AE Services software since CM 3.x has been End-Of-Manufacturer-Support as of December 2008.

Patch Notes

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

Backup before applying the patch

Please take a backup of AE Services database before applying AE Services 4.2.4 Super Patch 1.

Follow these steps to back up the AE Services database:

1. From your browser, log in to AE Services OAM.
2. From the main menu, select **CTI OAM Administratio**n to access the CTI OAM home page.
3. From the CTI OAM home page, click **Maintenance** > **Backup Database**.

   AE Services backs up the database, and displays the Database Backup page, that displays the following message:

   The backup file can be downloaded from **here**.
4. Click the "**here**" link.

   A file download dialog box is displayed, that allows you to either open or save the backup file (named as: mvapdb*ddmmyyyy*.tar.gz, where ddmmyyyy is a date stamp).
5. Click **Save**, and download the backup file to a safe location that the upgrade will not affect.

   For example, save the file to your local computer or another computer used for storing backups.

Download

To download the patch, go to:

1. http://support.avaya.com/download, and navigate to AE Services 4.2.x, then locate the entry **AE Services 4.2.4 Super Patch 1**.
2. PLDS, and list the downloads for Application Enablement Services (version 4.2 can be entered within the Advanced Search), then locate the entry **AE Services 4.2.4 Super Patch 1**.

Note: All AE Services Software Downloads are now to be found in PLDS, while the Release Notes documents are provided on the Support Site. There will be cross references between the corresponding download entries for patches.

File name	4.2.4_35SuperPatch1.zip
File size	49.7 MB (52,159,950 Bytes)
MD5 Sum	8ff9ce193b25a1e05c4a014e562bc9c1

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

Run the following from the command line:

```
md5sum 4.2.4_35SuperPatch1.zip
```

Note:

If the MD5 checksum does not match what is stated above, do not proceed with the installation of the patch. Download the patch and check the MD5 checksum again.

Patch install instructions | Service-interrupting?

Patch Installation Instructions for Bundled Server: Yes

1. Login as **sroot**. or **root**
2. Copy 4.2.4_35SuperPatch1.zip to **/tmp** directory on the Application Enablement Server.
3. Run the following from the command line:

   ```
   cd /tmp
   update -u 4.2.4_35SuperPatch1.zip
   ```
4. Follow the on-screen instructions.

After applying Super Patch 1, reboot the AE Server.

Post Patch Installation verification:

1. Login as **sroot**. or **root**

2. Run the following command to verify the installation of Super Patch 1:
   swversion
   The swversion command should return the following:

   ```
   ************* Patch Numbers Installed in this system are *************
   ====
   1
   ====
   ```

   In case you used swversion -a, the rpms will be listed as well below the patch number:

   ```
   ************* Patch Numbers Installed in this system are *************
   ====
   1
   mvap-platform-4.2.4.506-1.noarch.rpm
   ====
   ```
3. Log into AE Services OAM.
4. On the OAM home page, click **CTI OAM Administration**.
5. On the CTI OAM home page, verify that all previously licensed services are running.
6. Validate the server configuration data, as follows:
   - From the CTI OAM home page, click **Administration**.
   - Next, click **Network Configuration** >
   - Under **Local IP**, verify that the settings are correct.
   - Under **NIC Configuration**, verify that the settings are correct.
   - Under **Ports**, verify that the settings are correct.
7. Check all of the remaining OAM pages listed under Administration. Verify that the information is complete and correct.

This completes the installation of Super Patch 1.

Follow the procedure only if the AE Server configuration data has changed.

Follow this procedure to restore the database:

1. From the CTI OAM main menu, select **Maintenance** > **Restore Database**.

   OAM displays the Restore Database Configuration page. The initial state of the Restore Database page provides you with two basic functions:

   - Text box with the Browse button, which provides the means to select a backup file to use for the Restore process. Alternatively, you can type a fully qualified name of the backup file in the text box.
   - Restore button, that starts the Restore process
2. Click **Browse** and locate the AE Services database backup file that you intend to use

   (For example: mvapdb10012006.tar.gz).
3. Click **Restore**.

   OAM redisplays the Restore Database Configuration page, with the following message. "A database restore is pending. You must restart the Database Service and the AE Server for the restore to take effect. To restart these services now, click the Restart Services button below."
4. Click **Restart Services**.

   AE Services restarts the Database Service and the AE Server, thereby completing the Restore process.

Verification

The verification procedure is described within the "Patch Install Instructions" section.
Please make sure the patch was successfully applied before considering the Database Restore.

Failure

n/a

Patch uninstall instructions

Follow the **Patch Uninstall Instructions**:

1. Login as **sroot**. or **root**
2. Run the following from the command line:

   update -e 1

3. Follow the on-screen instructions.

After removing Super Patch 1, reboot the AE Server.

Do I have to perform any additional steps if I am uninstalling the Super Patch?
No.

Security Notes

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

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.