Product Support Notice

PSN #	PSN003406u				
Original publication date: 19-Sep-11. This is Issue #01, published date: 19-Sep-11.		Severity/risk level	High	Urgency	When convenient
Name of problem	Avaya Aura® System Platform Patch 6.0.3.3.3 for Avaya Aura System Platform 6.0.3.0.3 and 6.0.3.1.3				

Products affected

Avaya Aura Application Enablement (AE) Services running on Avaya Aura System Platform 6.0.3.0.3 or 6.0.3.1.3: Release 6.1.1

Problem description

This is a patch for System Platform 6.0.3.0.3 and 6.0.3.1.3.

This patch resolves the following issues:

Issue SP926311: Domain-0 memory leak due to Xen Libvirt

Resolution

Install System Platform Patch 6.0.3.3.3

Workaround or alternative remediation

n/a

Remarks

The system will automatically restart the System Platform WebConsole.

Patch 6.0.3.3.3 is a cumulative patch including updates from patch 6.0.3.1.3

Patch Notes

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

Backup before applying the patch

Highly Recommended

Download

To download the patch, go to:

A. Avaya Support (http://support.avaya.com/download), and navigate to the Avaya Aura Application Enablement Services product page. Select the Downloads link in the left-hand menu, change the dropdown box to 6.1.x, and then locate the entry, **Avaya Aura System Platform Patch 6.0.3.3.3** (new entries are inserted at the top of the list)

B. PLDS (https://plds.avaya.com) and select View Downloads. Use the search engine to locate the available downloads for Application Enablement Services using version 6.1 to narrow the search. Locate the entry, **Avaya Aura System Platform Patch 6.0.3.3.3** (new entries are inserted at the end of the list). Alternatively, you can search for the Download ID, which is **AES00000308**.

File Name	vsp-patch-6.0.3.3.3.noarch.rpm
File Size	201.18 MB (26,369,878 Bytes)
MD5 Sum	2be76776d633425c4c56fb8b87bc8e3b

Before you start with the installation of the Patch, check the md5 checksum of the file.
Run the following from the command line:

```
md5sum vsp-patch-6.0.3.3.3.noarch.rpm
```

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

Patch install instructions	Service-interrupting?
Patch installation instructions are available in the *Administering Avaya Aura™ System Platform* document available on Avaya Support (http://support.avaya.com/download).	Yes

Patch Installation Summary Instructions for System Platform:

1. Login to the System Platform (SP) Web Console,
2. Navigate to **Server Management | Patch Management | Download/Upload**
3. Choose the source of the patch (PLDS, HTTP, SP, devices on SP, or local to your PC).
4. Click the Search or Add button.

5. After it has been uploaded to SP, click on **Manage** (from the **Patch Management** menu). Now you will see the available patch waiting for installation below the section labeled **System Platform**.
6. Once you are ready, click on the **PatchID** link, finally on the **Install** button.
7. Follow the on-screen instructions.

Verification

Post Patch Installation Verification:

1. Log into the System Platform Web Console using a browser.
2. Navigate to **Server Management | Patch Management | Manage**
3. Check that the installed patch is listed under the **System Platform** section with a status of "Active".

Failure

Contact Technical Support

Patch uninstall instructions

The Patch can be uninstalled using the following instructions:

1. Login to the System Platform Web Console using a browser.
2. Navigate to **Server Management | Patch Management | Manage**. Now you will see the installed patch as active.
3. Click on the **PatchID** link, finally on the R**emove** button.
4. To also remove the patch file itself, click on the **Remove Patch File** button.

Note: This patch needs to be removed from an HA system while the Failover Mode is running.

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.