Product Support Notice

PSN #	PSN004304u			
Original publication date: 12-Nov-14. This is Issue #02, published date: 27-Nov-14.	Severity/risk level	Medium	Urgency	When convenient
Name of problem	Avaya Aura® Application Enablement (AE) Services 6.3.3 Linux Security Update Patch 1 Release Note			
Products affected				
Avaya Aura® Application Enablement (AE) Services Release 6.3.3 (Bundled, VMware, and System Platform offer types)				
Problem description				

What is fixed in this Patch?

This patch contains the following Red Hat Enterprise Linux 5.10 OS security updates:

Updated Package	Red Hat Advisory	Errata	Common Vulnerability and Exposure (CVE) ID
nss nspr	[RHSA-2013-1791] Important: nss and nspr security, bug fix, and enhancement update.	https://rhn.redhat.com/errata/RHSA-2013-1791.html	• Application level denial of service and/or arbitrary code execution (CVE-2013-5605, CVE-2013-1739, CVE-2013-1741, CVE-2013-5607) • Potential bypass of intended access restrictions (CVE-2013-5606)
	[RHSA-2013-1861] Moderate: nss security update.	https://rhn.redhat.com/errata/RHSA-2013-1861.html	Removal of intermediate certificate mis-issued by a subordinate Certificate Authority (Bugzilla#1038894)
	[RHSA-2014-0916] Critical: nss and nspr security update	https://rhn.redhat.com/errata/RHSA-2014-0916.html	Application level denial of service and/or arbitrary code execution (CVE-2014-1544)
	[RHSA-2014-1246] Moderate: nss and nspr security, bug fix, and enhancement update	https://rhn.redhat.com/errata/RHSA-2014-1246.html	• Potential disclosure of information (CVE-2013-1740) • Application level denial of service and/or arbitrary code execution (CVE-2014-1490, CVE-2014-1545) • Potential weak encryption (CVE-2014-1491) • Weak/incomplete certificate checking (CVE-2014-1492)
libtiff	[RHSA-2014-0223] Moderate: libtiff security update	https://rhn.redhat.com/errata/RHSA-2014-0223.html	Application level denial of service and/or arbitrary code execution (CVE-2013-1960, CVE-2013-4232, CVE-2013-4231, CVE-2013-4243, CVE-2013-4244, CVE-2013-1961) (Only applies to AES on System Platform)
httpd mod_ssl	[RHSA-2014-0369] Moderate: httpd security update	https://rhn.redhat.com/errata/RHSA-2014-0369.html	• Application level denial of service and/or arbitrary code execution, which can be remotely triggered if the vulnerable module is used, which is not the default on AES. (CVE-2013-6438) • Application level denial of service, which can be remotely triggered if a particular httpd option is enabled, which is not the default on AES. (CVE-2014-0098)

Updated Package	Red Hat Advisory	Errata	Common Vulnerability and Exposure (CVE) ID
gnutls	[RHSA-2014-0594] Important: gnutls security update	https://rhn.redhat.com/errata/RHSA-2014-0594.html	• Application level denial of service and/or arbitrary code execution (CVE-2014-3466, CVE-2014-3468) • Application level denial of service (CVE-2014-3467, CVE-2014-3469)
openssl	[RHSA-2014-0624] Important: openssl security update	https://rhn.redhat.com/errata/RHSA-2014-0624.html	Potential weak encryption (CVE-2014-0224)
	[RHSA-2014-1053] Moderate: openssl security update	https://rhn.redhat.com/errata/RHSA-2014-1053.html	• Potential disclosure of information (CVE-2014-3508) • Application level denial of service (CVE-2014-0221, CVE-2014-3505, CVE-2014-3506, CVE-2014-3510)
openssl097a	[RHSA-2014-0626] Important: openssl097a and openssl098e security update	https://rhn.redhat.com/errata/RHSA-2014-0626.html	Potential weak encryption (CVE-2014-0224)
glibc	[RHSA-2014-1110] Important: glibc security update	https://rhn.redhat.com/errata/RHSA-2014-1110.html	Arbitrary code execution (CVE-2014-5119, CVE-2014-0475)
openldap	[RHSA-2014-0206] Moderate: openldap security update	https://rhn.redhat.com/errata/RHSA-2014-0206.html	Application level denial of service (CVE-2013-4449)
krb5	[RHSA-2014-1245] Moderate: krb5 security and bug fix update	https://rhn.redhat.com/errata/RHSA-2014-1245.html	Application level denial of service (CVE-2014-4344, CVE-2014-434) **Note**: CVE-2013-1418 and CVE-2013-6800 are also included in this RHSA. These CVEs do not apply to AES.
kernel	[RHSA-2014-0433] Moderate: kernel security, bug fix, and enhancement update	https://rhn.redhat.com/errata/RHSA-2014-0433.html	• System level denial of service (CVE-2012-6638) • System level denial of service and/or privilege escalation (CVE-2013-2888)
	[RHSA-2014-0926] Moderate: kernel security and bug fix update	https://rhn.redhat.com/errata/RHSA-2014-0926.html	• Potential disclosure of information (CVE-2014-4021) • System level denial of service (CVE-2014-2678)
	[RHSA-2014-1143] Moderate: kernel security and bug fix update	https://rhn.redhat.com/errata/RHSA-2014-1143.html	Potential disclosure of information and/or system level denial of service (CVE-2014-3917)

Resolution

Install Linux Security Update 1 for AE Services 6.3.3

Workaround or alternative remediation

n/a

Remarks

1. What RHEL 5.10 RPMs are updated by Linux Security Update Patch 1?

glibc-2.5-123.i686.rpm

glibc-common-2.5-123.i386.rpm

gnutls-1.4.1-16.el5_10.i386.rpm

httpd-2.2.3-91.el5.i386.rpm

kernel-2.6.18-371.12.1.el5.i686.rpm (VMWare offer type only)

kernel-PAE-2.6.18-371.12.1.el5.i686.rpm (Bundled offer type only)

kernel-headers-2.6.18-371.12.1.el5.i386.rpm (System Platform offer type only)

kernel-xen-2.6.18-371.12.1.AV2.domU.el5.i686.rpm (System Platform offer type only)
krb5-libs-1.6.1-80.el5_11.i386.rpm
krb5-workstation-1.6.1-80.el5_11.i386.rpm
libtiff-3.8.2-19.el5_10.i386.rpm (VMWare and System Platform offer type only)
mod_ssl-2.2.3-91.el5.i386.rpm
nscd-2.5-123.i386.rpm
nspr-4.10.6-1.el5_10.i386.rpm
nss-3.16.1-2.el5.i386.rpm
openldap-2.3.43-28.el5_10.i386.rpm
openldap-clients-2.3.43-28.el5_10.i386.rpm
openldap-servers-2.3.43-28.el5_10.i386.rpm
openldap-servers-overlays-2.3.43-28.el5_10.i386.rpm
openssl-0.9.8e-27.el5_10.4.i386.rpm
openssl097a-0.9.7a-12.el5_10.1.i386.rpm
ti_usb_3410_5052-1.28-1.AV12.i386.rpm (Bundled offer type only)

2. Is applying Linux Security Update Patch 1 service affecting?
Yes, the AE Services server will be rebooted once the install completes.

3. With which Application Enablement Services release(s) and offer type(s) is Linux Security Update Patch 1 compatible?
This patch is compatible with the AE Services 6.3.3 Bundled, VMware and System Platform offer types.

4. Is the Linux Security Update Patch 1 cumulative?
This is the first AE Services 6.3.3 Linux Security Update patch to be released.
Note: The Bash Shellshock security patch is a separate security patch associated with PSN004303u.
Note: This Linux Security Update patch is installed independent of any AE Services Super Patch.

5. Is the Linux Security Update Patch 1 compatible with Application Enablement Services 5.x, 6.1.x, 6.3.0, or 6.3.1 servers?
No. The Linux Security Update Patch 1 is only supported with AE Services 6.3.3.

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 the AE Services server data before applying the Linux Security Update Patch.

Follow these steps to back up the AE Services server data:

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 **Database Backup** screen, that displays the following message:
   The backup file can be downloaded from **Here**.
3. Click the "**Here**" link.
   A file download dialog box is displayed, that allows you to either open or save the backup file (named as: *serverName*_r*SoftwareVersion*_mvapdb*ddmmyyyy*.tar.gz, where ddmmyyyy is a date stamp).
4. 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 AE Services patch, go to:

A. Avaya Support (http://support.avaya.com/downloads). On the “Downloads” screen, in the textbox labeled “Enter Product Name”, enter “Avaya Aura Application Enablement Services” and the release option “6.3.x”. If the option “Select a content type” is displayed select the “Download” radio button and click the button labeled “Enter”. If the Documents table is displayed, select the link, “View downloads”, on the right-hand side of the screen above the Documents table. In the

Downloads table locate and select the entry, **Avaya Aura® Application Enablement Services 6.3.3 Linux Security Update Patch 1** (new entries are inserted at the top of the list).

B. PLDS (https://plds.avaya.com). Select View Downloads. Use the search engine to locate the available downloads for Application Enablement Services using version 6.3 to narrow the search. Locate the entry, **Avaya Aura® Application Enablement Services 6.3.3 Linux Security Update Patch 1** (new entries are inserted at the end of the list). Alternatively, you can search for the Download ID, which is **AES00000490.**

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

File Name	633_LSUPatch1.bin
File Size	93.5205 MB (93520466 Bytes)
MD5 Sum	57856d1a9b38201b4bffc0f095de3789

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

```
md5sum 633_LSUPatch1.bin
```

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?
How to check the detailed AE Services version	Yes

A. For the AE Services on System Platform offer, use the System Platform Management Console (and hence see whether the patch has been applied already):

1. Log into the System Platform Management Console using a browser.
2. Go to **Virtual Machine Management | Manage** (that is the page which should come up after connecting to the web console)
3. Verify that your AE Services VM has AE Services 6.3.3 running (the GA version shows 6.3.3.0.10)
4. Click on that version information to get the detailed version information in a popup window.
5. If the patch, LSU-6.3.3-1, is not listed, continue to the next section, "**How to install the Patch to the AE Services server**".

   Note:
   When multiple patches for the AE Services server is installed, the System Platform Management Console may show each of the installed patches as "Active" instead of only showing the latest installed patch as "Active" and the previous installed patches as "Installed". While other VM's may use a patch status consisting of "Active", "Installed" and "Uninstalled", AE Services currently only use the patch status "Active" and "Uninstalled".

B. For the Bundled and VMware offer, use the AE Services Linux console (and hence see whether the patch has been applied already):

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using e.g. putty or SSH)
2. As the root user, execute the following command: **swversion**
3. If the patch, LSU-6.3.3-1, is not listed, continue to the next section, "**How to install the Patch to the AE Services server**".

How to install the Patch on the AE Services server.

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. Secure copy **633_LSUPatch1.bin** to the **/tmp** directory on the AE Services server.
3. As the root user, execute the following from the command line:
   ```
   cd /tmp
   chmod 750 633_LSUPatch1.bin
   ./633_LSUPatch1.bin
   ```
4. Follow the on-screen instructions.

   Note: The AE Services server will be rebooted as part of the patch install process.

Verification

Post Patch Installation Verification:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely, using e.g. putty)
2. Login as **sroot** or **root**
3. Run the following command to verify the installation of Linux Security Update Patch 1:
   ```
   swversion
   ```

   The swversion command should return something similar to the following if Linux Security Update Patch 1 is installed:
   ```
   ************* Patch Numbers Installed in this system are *************
   ====
   LSU-6.3.3-1
   ====
   ```

   In case you used **swversion -a,** the RPMs will be listed as well below the patch number – this is the 6.2.0 possible output:
   ```
   ************** Patches Installed in this system are  ***************
   ====
   LSU-6.3.3-1
   glibc-2.5-123.i686.rpm
   glibc-common-2.5-123.i386.rpm
   gnutls-1.4.1-16.el5_10.i386.rpm
   httpd-2.2.3-91.el5.i386.rpm
   krb5-libs-1.6.1-80.el5_11.i386.rpm
   krb5-workstation-1.6.1-80.el5_11.i386.rpm
   mod_ssl-2.2.3-91.el5.i386.rpm
   nscd-2.5-123.i386.rpm
   nspr-4.10.6-1.el5_10.i386.rpm
   nss-3.16.1-2.el5.i386.rpm
   openldap-2.3.43-28.el5_10.i386.rpm
   openldap-clients-2.3.43-28.el5_10.i386.rpm
   openldap-servers-2.3.43-28.el5_10.i386.rpm
   openldap-servers-overlays-2.3.43-28.el5_10.i386.rpm
   openssl-0.9.8e-27.el5_10.4.i386.rpm
   openssl097a-0.9.7a-12.el5_10.1.i386.rpm
   kernel-2.6.18-371.12.1.el5.i686.rpm  (VMWare offer type only)
   kernel-PAE-2.6.18-371.12.1.el5.i686.rpm  (Bundled offer type only)
   kernel-headers-2.6.18-371.12.1.el5.i386.rpm  (System Platform offer type only)
   kernel-xen-2.6.18-371.12.1.AV2.domU.el5.i686.rpm  (System Platform offer type only)
   libtiff-3.8.2-19.el5_10.i386.rpm  (VMWare and System Platform offer type only)
   ti_usb_3410_5052-1.28-1.AV12.i386.rpm  (Bundled offer type only)
   ====
   ```

   Note: Instead of the steps 1 - 3 as listed above, you can use the same procedure as described in the Patch install instructions section for AE Services on System Platform (which does not require a console login).

4. Login to the AE Services Management Console using a browser.
5. From the main menu, click **Status**.
6. On the Status page, verify that all previously licensed services are running.
7. Validate the server configuration data, as follows:
   - From the main menu, click **Networking**.
   - Under **AE Service IP (Local IP)**, verify that the settings are correct.
   - Under **Network Configure**, verify that the settings are correct.
   - Under **Ports**, verify that the settings are correct.
8. Check all of the remaining Management Console pages listed under **AE Services** and **Communication Manager Interface**. Verify that the information is complete and correct.

This completes the installation of the Patch.

Follow this procedure only if the AE Services server configuration data has changed.

Follow this procedure to restore the AE Services server data:

1. From the main menu of the AE Services Management Console, select **Maintenance | Server Data | Restore**.
   The Management Console displays the Restore Database Configuration screen. 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: serverName_r6-3-3-10-0_mvapdb01012014.tar.gz).
3. Click **Restore**.
   The Management Console 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 Services, thereby completing the Restore process.

Failure

n/a

Patch uninstall instructions

A Linux Security Update patch 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

This issue affects all products which use the Bash shell and parse values of environment variables. This issue is especially dangerous as there are many possible ways Bash can be called by an application. Quite often if an application executes another binary, Bash is invoked to accomplish this. Because of the pervasive use of the Bash shell, this issue is quite serious and should be treated as such.

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

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.

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.