Product Support Notice

PSN # PSN003992u

Original publication date: 17-Jun-13. This is Issue #01, published date: 17-Jun-13. | Severity/risk level | Medium | Urgency | When convenient

Name of problem | Avaya Aura® Application Enablement (AE) Services 6.2.0 Linux Security Update Patch 1 Release Note

Products affected

Avaya Aura Application Enablement (AE) Services Release 6.2.0 (all offer types)

Problem description

What is fixed in this Patch?

This patch contains the following Red Hat Enterprise Linux 5.7 OS security updates:

Red Hat Advisory	Errata	Common Vulnerability and Exposure (CVE) ID
[RHSA-2012:0397-01] Moderate: glibc security update	https://rhn.redhat.com/errata/RHSA-2012-0397.html	Arbitrary code execution bypassing standard security protections (CVE-2012-0864)
[RHSA-2012:0428-01] Important: gnutls security update	https://rhn.redhat.com/errata/RHSA-2012-0428.html	Application level denial-of-service and/or arbitrary code execution (CVE-2012-1573, CVE-2012-1569, CVE-2011-4128)
[RHSA-2012:0426-01] Moderate: openssl security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-0426.html	Application level denial-of-service (CVE-2012-1165) Potential disclosure of information related to encryption keys (CVE-2012-0884)
[RHSA-2012:0451-01] Important: rpm security update	https://rhn.redhat.com/errata/RHSA-2012-0451.html	Application level denial-of-service and/or arbitrary code execution (CVE-2012-0060, CVE-2012-0061,CVE-2012-0815)
[RHSA-2012:0467-01] Important: freetype security update	https://rhn.redhat.com/errata/RHSA-2012-0467.html	Application level denial-of-service and/or arbitrary code execution (CVE-2012-1134, CVE-2012-1136, CVE-2012-1142, CVE-2012-1126, CVE-2012-1127, CVE-2012-1130, CVE-2012-1131, CVE-2012-1132, CVE-2012-1137, CVE-2012-1139, CVE-2012-1140, CVE-2012-1141, CVE-2012-1143)
[RHSA-2012:0480-01] Important: kernel security, bug fix, and enhancement update	https://rhn.redhat.com/errata/RHSA-2012-0480.html	System level denial-of-service which can be triggered remotely if the vulnerable kernel module is loaded, which is not the default on AES. (CVE-2012-1583)
[RHSA-2012:0518-01] Important: openssl security update	https://rhn.redhat.com/errata/RHSA-2012-0518.html	Application level denial-of-service and/or arbitrary code execution (CVE-2012-2110)
[RHSA-2012:0678-01] Moderate: postgresql and postgresql84 security update	https://rhn.redhat.com/errata/RHSA-2012-0678.html	Privilege escalation (CVE-2012-0868, CVE-2012-0866) Weak/incomplete certificate checking (CVE-2012-0867)
[RHSA-2012:0690-01] Important: kernel security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-0690.html	System level denial-of-service and/or privilege escalation (CVE-2012-2136)
[RHSA-2012:0699-01] Moderate: openssl security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-0699.html	Application level denial-of-service (CVE-2012-2333)

Red Hat Advisory	Errata	Common Vulnerability and Exposure (CVE) ID
[RHSA-2012:0716-01] Important: bind security update	https://rhn.redhat.com/errata/RHSA-2012-0716.html	Application level denial-of-service and potential disclosure of information (CVE-2012-1667, CVE-2012-1033)
PostgreSQL Security Updates	http://www.postgresql.org/about/news/1377/	Weak password hashing (CVE-2012-2143) Potential Information disclosure (CVE-2012-3488, CVE-2012-3489)
[RHSA-2012:0720-01] Important: kernel security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-0720.html	Arbitrary code execution with escalated privileges (CVE-2012-0217) System-level denial-of-service (CVE-2012-1583)
[RHSA-2012:0745-01] Moderate: python security update	https://rhn.redhat.com/errata/RHSA-2012-0745.html	Application level denial-of-service (CVE-2012-1150)
[RHSA-2012:0731-01] Moderate: expat security update	https://rhn.redhat.com/errata/RHSA-2012-0731.html	Application level denial-of-service (CVE-2012-0876)
[RHSA-2012:1054-01] Important: libtiff security update	https://rhn.redhat.com/errata/RHSA-2012-1054.html	Application level denial-of-service and/or arbitrary code execution (CVE-2012-2088, CVE-2012-2113) (Only applies to AES on System Platform)
[RHSA-2012:1061-01] Moderate: kernel security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-1061.html	System-level denial-of-service (CVE-2012-3375)
[RHSA-2012:1081-01] Moderate: sudo security update	https://rhn.redhat.com/errata/RHSA-2012-1081.html	Remote privilege escalation (CVE-2012-2337)
[RHSA-2012:1087-01] Important: kernel security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-1087.html	System level denial-of-service and/or privilege escalation (CVE-2012-2136)
[RHSA-2012:1090-01] Moderate: nss and nspr security, bug fix, and enhancement update	https://rhn.redhat.com/errata/RHSA-2012-1090.html	Application level denial-of-service (CVE-2012-0441)
[RHSA-2012:1149-01] Moderate: sudo security and bug fix update	https://rhn.redhat.com/errata/RHSA-2012-1149.html	Privilege escalation (CVE-2012-3440)
[RHSA-2012:1512-01] Important: libxml2 security update	https://rhn.redhat.com/errata/RHSA-2012-1512.html	Application level denial-of-service and/or arbitrary code execution (CVE-2012-5134)
[RHSA-2013:0122-01] Moderate: tcl security and bug fix update	https://rhn.redhat.com/errata/RHSA-2013-0122.html	Application level denial-of-service (CVE-2007-4772, CVE-2007-6067)
[RHSA-2013:0130-01] Low: httpd security, bug fix, and enhancement update	https://rhn.redhat.com/errata/RHSA-2013-0130.html	Input sanitization flaws (CVE-2008-0455, CVE-2008-0456, CVE-2012-2687)

Resolution

Install Linux Security Update 1 for AE Services 6.2.0

Workaround or alternative remediation

n/a

Remarks

1. What RHEL 5.7 RPMs are updated by Linux Security Update Patch 1?

bind-libs-9.3.6-20.P1.el5_8.6.i386.rpm
bind-utils-9.3.6-20.P1.el5_8.6.i386.rpm
dbus-glib-0.73-11.el5_9.i386.rpm
expat-1.95.8-11.el5_8.i386.rpm
freetype-2.2.1-32.el5_9.1.i386.rpm
glibc-2.5-107.i686.rpm
glibc-common-2.5-107.i386.rpm
nscd-2.5-107.i386.rpm
gnutls-1.4.1-10.el5_9.1.i386.rpm
httpd-2.2.3-76.el5_9.i386.rpm
mod_ssl-2.2.3-76.el5_9.i386.rpm
kernel-headers-2.6.18-348.3.1.el5.i386.rpm
kernel-xen-2.6.18-348.3.1.AV2.domU.el5.i686.rpm
libpng-1.2.10-17.el5_8.i386.rpm
libtiff-3.8.2-18.el5_8.i386.rpm
libxml2-2.6.26-2.1.21.el5_9.2.i386.rpm
libxslt-1.1.17-4.el5_8.3.i386.rpm
nspr-4.9.2-2.el5_9.i386.rpm
nss-3.13.6-3.el5_9.i386.rpm
openssl-0.9.8e-26.el5_9.1.i386.rpm
pango-1.14.9-8.el5_7.3.i386.rpm
postgresql-8.1.23-6.el5_8.i386.rpm
postgresql-libs-8.1.23-6.el5_8.i386.rpm
postgresql-server-8.1.23-6.el5_8.i386.rpm
python-2.4.3-56.el5.i386.rpm
python-libs-2.4.3-56.el5.i386.rpm
rpm-4.4.2.3-32.el5_9.i386.rpm
rpm-libs-4.4.2.3-32.el5_9.i386.rpm
popt-1.10.2.3-32.el5_9.i386.rpm
sudo-1.7.2p1-22.el5_9.1.i386.rpm
tcl-8.4.13-6.el5.i386.rpm
wget-1.11.4-3.el5_8.2.i386.rpm
elinks-0.11.1-8.el5_9.i386.rpm

2. Is applying Linux Security Update Patch 1 service affecting?

Yes, the AE Services server will need to be rebooted after the patch is applied.

3. With which Application Enablement Services release(s) is Linux Security Update Patch 1 compatible?

This patch is compatible with all AE Services 6.2.0 offer types.

4. Is the Linux Security Update Patch 1 cumulative?

N/A, this is the first patch to be released.

5. Is the Linux Security Update Patch 1 compatible with Application Enablement Services 5.x or 6.1.x servers?

No. The Linux Security Update Patch 1 is only supported with AE Services 6.2.0.

6. Is the Linux Security Update Patch 1 available for all Offer Types?

Yes. Please use the appropriate procedure for the upgrade, i.e. via the Patch Management menu in the web console of the System Platform for Virtual Appliance offer and directly on the AE Services server for Bundled or Software Only systems.

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 Linux Security Update patch, go to:

A. Avaya Support (http://support.avaya.com/downloads). On the "Downloads and Documents" screen, in the textbox labeled "Enter Your Product Here", enter "Avaya Aura Application Enablement Services" and the release option "6.2.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 6.2.0 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 6.2 to narrow the search. Locate the entry, **Avaya Aura® Application Enablement Services 6.2.0 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 **AES00000428**.

Note:
All AE Services Software Downloads are now 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	620_LSUPatch1.bin
File Size	84.99 MB (89,120,598 Bytes)
MD5 Sum	6f60128ac30cfe63d41fc7c235dc84b1

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

md5sum 620_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 6.2.0 running (the GA version shows 6-2-0-

18)

4. Click on that version information to get the detailed version information in a popup window.
5. If the patch 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 Software Only 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 is not listed, continue to the next section, "**How to install the Patch to the AE Services server**".

How to install the Patch to the AE Services server.

A. Patch Installation Instructions for the AE Services on System Platform offer

1. On the System Platform (SP) Management Console, click on **Server Management | Patch Management | Download/Upload**
2. Choose the source of the patch (PLDS, HTTP, SP, devices on SP, or local to your PC).
3. 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 caption **AES**.
4. Once you're ready, click on the **PatchID** link, finally on the **Install** button.
5. Follow the on-screen instructions.

B. Patch Installation Instructions for the Bundled or Software Only offer:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using e.g. putty or SSH)
2. Secure copy **620_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
   update -u --force 620_LSUPatch1.bin
4. Follow the on-screen instructions.

After applying the Linux Security Update Patch, the AE Services server will reboot.

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 **********
====
LSU1
====

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 **********
====
LSU1
bind-libs-9.3.6-20.P1.el5_8.6.i386.rpm
bind-utils-9.3.6-20.P1.el5_8.6.i386.rpm
dbus-glib-0.73-11.el5_9.i386.rpm
expat-1.95.8-11.el5_8.i386.rpm
freetype-2.2.1-32.el5_9.1.i386.rpm
glibc-2.5-107.i686.rpm
glibc-common-2.5-107.i386.rpm
nscd-2.5-107.i386.rpm
gnutls-1.4.1-10.el5_9.1.i386.rpm
httpd-2.2.3-76.el5_9.i386.rpm
mod_ssl-2.2.3-76.el5_9.i386.rpm
kernel-headers-2.6.18-348.3.1.el5.i386.rpm
kernel-xen-2.6.18-348.3.1.AV2.domU.el5.i686.rpm
libpng-1.2.10-17.el5_8.i386.rpm
libtiff-3.8.2-18.el5_8.i386.rpm
libxml2-2.6.26-2.1.21.el5_9.2.i386.rpm
libxslt-1.1.17-4.el5_8.3.i386.rpm
nspr-4.9.2-2.el5_9.i386.rpm
nss-3.13.6-3.el5_9.i386.rpm
openssl-0.9.8e-26.el5_9.1.i386.rpm
pango-1.14.9-8.el5_7.3.i386.rpm
postgresql-8.1.23-6.el5_8.i386.rpm
postgresql-libs-8.1.23-6.el5_8.i386.rpm
postgresql-server-8.1.23-6.el5_8.i386.rpm
python-2.4.3-56.el5.i386.rpm
python-libs-2.4.3-56.el5.i386.rpm
rpm-4.4.2.3-32.el5_9.i386.rpm
rpm-libs-4.4.2.3-32.el5_9.i386.rpm
popt-1.10.2.3-32.el5_9.i386.rpm
sudo-1.7.2p1-22.el5_9.1.i386.rpm
tcl-8.4.13-6.el5.i386.rpm
wget-1.11.4-3.el5_8.2.i386.rpm
elinks-0.11.1-8.el5_9.i386.rpm
====

> **Note**: Instead of the steps 1 - 3 as listed above, you can use the same procedure as described at the beginning of this 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_r6-2-0-18-0_mvapdb01012013.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.

Verification

See the **Post Patch Installation Verification** section above.

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

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