



Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN # PSN004303u

Original publication date: 09-Oct-14. This is Issue #04, published date: 31-Mar-15.

Severity/risk level

High

Urgency

Immediately

Name of problem Avaya Aura® Application Enablement (AE) Services Bash Shellshock Security Patch Release Notes

Products affected

Avaya Aura® Application Enablement (AE) Services Release 5.x and 6.x (all offer types)

Problem description

This security patch contains the following security update:

Red Hat has issued a security vulnerability notice affecting all versions of the Bash package as shipped with Red Hat products. The GNU Bourne Again shell (Bash) is a shell and command language interpreter compatible with the Bourne shell (sh). Bash is the default shell for Red Hat Enterprise Linux.

A flaw was found in the way Bash evaluated certain specially crafted environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Certain services and applications allow remote unauthenticated attackers to provide environment variables, allowing them to exploit this issue.

References:

- Bash Code Injection Vulnerability via Specially Crafted Environment Variables (CVE-2014-6271, CVE-2014-7169) <https://access.redhat.com/articles/1200223>
- Resolution for Bash Code Injection Vulnerability via Specially Crafted Environment Variables (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278) in Red Hat Enterprise Linux <https://access.redhat.com/node/1207723>
- Red Hat Advisory RHSA-2014:1306-3 <https://rhn.redhat.com/errata/RHSA-2014-1306.html>

Resolution

For AE Services 5.2.x and 6.x, install the self-executable security patch, “aesvcs_bash_patch.bin”. This security patch is customer installable.

Note: It is highly recommended to upgrade any AE Services release older than AE Services 5.2.4 to a newer release.

Note: Unless otherwise stated in a future PSN

- The Bash security patch does not need to be reinstalled, when an AE Services SuperPatch or Linux Security Update patch is applied to the AE Services server.
- The Bash security patch will need to be reinstalled, when the AE Services server is upgraded to a newer AE Services 5.x or 6.x release.
- The Verification section in this PSN can be used to verify if the correct bash RPM is installed after applying an AE Services upgrade or update.

Workaround or alternative remediation

n/a

Remarks

1. What is installed by aesvcs_bash_patch.bin?

bash-3.2-33.el5_11.4.AV1.i386.rpm

2. Is applying aesvcs_bash_patch.bin 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 aesvcs_bash_patch.bin compatible?

The aesvcs_bash_patch.bin security patch is compatible with all AE Services 5.2.x and 6.x offer types, except SW Only. All SW Only solutions need to obtain the Bash RPM from their Red Hat vendor.

4. Is the Bash RPM installed by aesvcs_bash_patch.bin cumulative?

Yes, the Bash RPM includes all the previous Bash RPM modifications from Red Hat.

Note: This Linux Security Update patch is installed independent of any AE Services SuperPatch.

Patch Notes

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

Backup before applying the patch

n/a

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 “5.2.x” or one of the available 6.x options. 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® AE Services 5.2.4 and 6.x Bash Shellshock Remediation** (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 the appropriate 5.2 or 6.x version to narrow the search. Locate the entry, **Avaya Aura® AE Services 5.2.4 and 6.x Bash Shellshock Remediation** (new entries are inserted at the end of the list). Alternatively, you can search for the Download ID, which is **AES00000489**

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	aesvcs_bash_patch.bin
File Size	1.849 MB (1849101 Bytes)
MD5 Sum	0fadf526ce34156d2d1a94853ec3ba5c

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

Run the following from the command line:

```
md5sum aesvcs_bash_patch.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 install the Bash security patch on the AE Services server.

Yes

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. Secure copy **aesvcs_bash_patch.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 aesvcs_bash_patch.bin  
./aesvcs_bash_patch.bin
```
4. Follow the on-screen instructions.

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

Verification

How to verify the Bash security patch is installed:

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. Execute the command “**swversion**”.
3. Verify the list of installed patches contain “**LSU-bash-shellshock**”.

How to verify the Bash RPM version was updated:

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. As a root user, execute the command “**rpm -qa | grep bash**”
3. Verify the installed bash version number is **bash-3.2-33.el5_11.4.AV1**.

How to verify the Bash issue has been resolved:

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. Execute the following command:
env 'x=() { :}; echo vulnerable' 'BASH_FUNC_x=() { :}; echo vulnerable' bash -c "echo test"
3. Verify the issues associated with CVE-2014-6271, RHSA-2014:1306, RHSA-2014:1311 and RHSA-2014:1312 has been resolved. If the output of the above command contains a line containing only the word vulnerable you are using a vulnerable version of Bash. Otherwise, this patch fixes this issue and ensures that no code is allowed after the end of a Bash function.
 - **Sample output if vulnerable:**
vulnerable
bash: BASH_FUNC_x(): line 0: syntax error near unexpected token `)`
bash: BASH_FUNC_x(): line 0: `BASH_FUNC_x() () { :}; echo vulnerable'
bash: error importing function definition for `BASH_FUNC_x'
test
 - **Sample output if resolved:**
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `BASH_FUNC_x'
test
4. Execute the following command:
cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>' bash -c "echo date"; cat /tmp/echo
5. Verify the issue associated with CVE-2014-7169 has been resolved. If your system is vulnerable, the time and date information will be displayed on the screen and a file called “/tmp/echo” will be created. Otherwise, this patch fixes this issue and ensures that the system is protected from the file creation issue.
 - **Sample output if vulnerable:**
bash: x: line 1: syntax error near unexpected token `='
bash: x: line 1: `
bash: error importing function definition for `x'
Fri Sep 26 11:49:58 GMT 2014
 - **Sample output if resolved:**
date
cat: /tmp/echo: No such file or directory

Failure

n/a

Patch uninstall instructions

This patch should not be removed.

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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.