



Product Support Notice

© 2014 Avaya Inc. All Rights Reserved.

PSN # PSN004321u

Original publication date: 9-Oct-2014. This is Issue #01, published date: 9-October-2014.

Severity/risk level

High

Urgency

Immediately

Name of problem AACC 6.4 SP13: Resolution of Shellshock bash Vulnerability for Red Hat Based AMS Installations

Products affected

Avaya Aura Contact Center (AACC): Release 6.4 SIP SP13 using Avaya Media Server (AMS) on Linux only.

Problem description

Shellshock bash vulnerability impacts Linux AMS installations only. Red Hat Enterprise Server Linux 5.x and 6.x patches are required to resolve the OS impact. AMS Software does NOT need to be updated. The vulnerability has the following assigned Red Hat RHN references: **CVE-2014-6277, CVE-2014-7169, CVE-2014-7186**

This issue is reported in the following wi:

wi01191043: bash RHEL vulnerability CVE-2014-6277, CVE-2014-7169, CVE-2014-7186. RPM update required for RHEL AACC 6.4 SP13 AMS OVA

Resolution

This resolution to this issue is as follows:

Avaya Media Server Software:

The Avaya Media Server Software for Red Hat Linux application does **not** have bash libraries built into the product so the AMS software does not need to be updated. However the Red Hat 5.x and 6.x 32bit and 64bit Operating Systems are impacted. Red Hat has released updated bash RPMs for all versions of Red Hat.

Operating System:

Windows 2008 is not affected by the Shellshock bash vulnerability, so no action is required on Windows AMS Servers.

All AMS supported versions of Red Hat Linux (5.x 32bit, 6.x 32bit and 64bit) are affected by the Shellshock vulnerability. The following section details the upgrade steps required depending on the AMS deployed solution

AMS Installed on Customer Purchased Red Hat Enterprise Server 5.x and Installed on Physical Server or on a VMWare Guest:

1. The customer is responsible for obtaining the updated bash RPM package that resolves the shellshock vulnerability: **bash-3.2-33.el5_11.4**. This can be obtained by registering your server on the Red Hat Network.
2. Install this RPM and reboot the Server.

AMS Installed on Customer Purchased Red Hat Enterprise Server 6.x and Installed on Physical Server or on a VMWare Guest:

1. The customer is responsible for obtaining the updated bash RPM package that resolves the shellshock vulnerability: **bash-4.1.2-15.el6_5.2**. This can be obtained by registering your server on the Red Hat Network.
2. Install this RPM and reboot the Server.

AACC SP13 AMS OVA Installed on VMWare ESXi:

1. AMS OVA shipped with AACC 6.4 SP13 containing the Shellshock vulnerability. Avaya is responsible for supplying this RPM for OVA customers. This update is supplied in the QFE: **QFE-__sip-conf-6.4.0.137-0003** which is available on support.avaya.com. This QFE must be applied to the SP13 AMS OVA Installation.
2. Reboot the Server.

Workaround or alternative remediation

n/a

Remarks

n/a

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	
n/a	
Patch install instructions	Service-interrupting?
n/a	Yes
Verification	
n/a	
Failure	
n/a	
Patch uninstall instructions	
n/a	

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

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.