Product Support Notice

© 2014 Avaya Inc. All Rights Reserved.

PSN #	PSN004209u				
Original publication date: 29-Sept-14. This is Issue #02, published date: 21-Oct-14.		Severity/risk level	Medium	Urgency	Immediately

Name of problem CMS Linux rpm update for bashbug/shellshock

Products affected

All R17 CMS Servers on the Linux Platforms

Problem description

CMS R17 Linux uses bash shell for many portions of the OS. The bashbug (Shellshock) vulnerability found with bash is resolved with the application of an updated rpm for the bash shell.

NOTE: CMS systems on Solaris operating systems are NOT affected. CMS systems on Solaris do NOT load the bash shell package and are not affected.

Resolution

This rpm will be incorporated into R17 R4.

Workaround or alternative remediation

This patch is customer installable. Customers may also contact their Avaya support organization or business partner regarding the installation of this patch. Installation by Avaya *is billable at current per incident rates.*

This patch can be installed following the instructions below:

For Linux systems:

1. Download bash-4.1.2-15.el6_5.2.x86_64.rpm from https://support.avaya.com/downloads/download-details.action?contentId=C2014926124599420_2&productId=P0030&releaseId=17.0.x to /tmp on the CMS system.

2. Check the md5 sum of the downloaded file. It should be 7dfec6a0e0368bed638dedd9b88e5596

```
Prompt> cd /tmp
Prompt> md5sum bash-4.1.2-15.el6_5.2.x86_64.rpm
       7dfec6a0e0368bed638dedd9b88e5596 bash-4.1.2-15.el6_5.2.x86_64.rpm
```

3. Install the rpm

```
Prompt> rpm –Uvh bash-4.1.2-15.el6_5.2.x86_64.rpm
```

4. A reboot is recommended, but not required.

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

yes

Download

bash-4.1.2-15.el6_5.2.x86_64.rpm

Patch install instructions	Service-interrupting?
n/a	No

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

Medium

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.