



Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN # PSN004297u

Original publication date: 30-Sep-14. This is Issue #03, published date: 22-May-15.

Severity/risk level

High

Urgency

Immediately

Name of problem CS 1000 R7.6 and R7.5 – “Shell Shock” Vulnerability Service Updates

Products affected

Communications Server 1000M and Communications Server 1000E – R7.6 and R7.5

Problem description

Introduction

(This PSN is updated May 2015 to reflect a change of location in ESPL for one Service Update (SU), as well as to correct AMS version information – there is no change in actual SU content on ESPL).

This PSN is issued to advise of recommended Service Updates for Communication Server 1000 R7.6 and R7.5 systems in response to the “Shell Shock” security vulnerability discovered in the Bash Shell for UNIX, Linux and OSX systems.

More information on the vulnerability can be found here:

<https://www.us-cert.gov/ncas/alerts/TA14-268A>

<https://access.redhat.com/security/cve/CVE-2014-6271>

<https://access.redhat.com/security/cve/CVE-2014-7169>

The relevant Service Updates are as follows and can be downloaded by partners via ESPL:

<https://espl.avaya.com/espl>

ESPL

Main Menu

Section: Serviceability Updates and Loadware/Firmware Distribution Tools (CS1000)

SU/LW/FW File Search

<next page>

Product: Linux

Release: 7.65.16.00 (R7.6), 7.65.16.26 (R7.6 with AMS 7.6) or 7.50.17.00 (R7.5)

Application: LinuxOS

- CS1000 Linux Base R7.6
 - o bash-3.2-33.el5_11.4.i386
- CS1000 Linux Base for AMS 7.6
 - o bash-3.2-33.el5_11.4.x86_64
- CS1000 Linux Base R7.5
 - o bash-3.2-33.el5_11.4.i386.075

Resolution

Apply recommended Service Updates – in case of R7.6 or R7.5.

There is no resolution in case of earlier software releases.

Workaround or alternative remediation

Not Applicable

Remarks

Not Applicable

Patch Notes

Backup before applying the patch

Data dump as before any maintenance activity

Download

Service Updates can be downloaded via ESPL

Patch install instructions	Service-interrupting?
As per standard documentation for CS 1000	No
Verification	
Not Applicable	
Failure	
Not Applicable	
Patch uninstall instructions	
Not Applicable	

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

This PSN is in response to the “Shell Shock” vulnerability as noted above.

Avaya Security Vulnerability Classification

Medium

Mitigation

Apply recommended Service Updates.

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.