Product Support Notice

PSN #	PSN027007u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.		
Original publication date: 07-Oct-14. This is Issue #4, published date: 24-Nov-14.	Severity/risk level	High	Urgency	Immediately
Name of problem	PSN027007u –System Platform update for the Bash shell vulnerability (Shellshock)			

Products affected

Avaya Aura® System Platform 6.0.3.x, 6.2.x, 6.3.x
S8800 Server
S8300 Server
Common Servers (HP & Dell)

Problem description

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 and CentOS. 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.
Please see Avaya Security Alert, ASA-2014-369, for more details.
https://downloads.avaya.com/css/P8/documents/100183009

Note: System Platform 6.2.x and 6.3.x install with a third and separate virtual machine known as SVM (Services VM).
This PSN does not cover that virtual machine. Please see the published Avaya Security Alert ASA-2014-377 to address the Bash shell vulnerability in the Services Virtual Machine.
https://downloads.avaya.com/css/P8/documents/100183066

Resolution

The following procedure should be applied to any System Platform 6.0.3.x or later server to address the Bash shell vulnerability (Shellshock).

The update will be included in the future System Platform Service Pack 6.3.6.

This update only addresses the vulnerability in System Platform. Any applications running on top of System Platform must be addressed separately. Refer to ASA-2014-369.

You will need to download the Avaya Aura® System Platform Bash shell vulnerability (Shellshock) update.

This self-extracting executable script is posted on PLDS under System Platform, PLDS Download ID SP00000040.

The following procedure should be applied to any System Platform 6.0.3.x system or later system.

While this procedure is not service affecting, it is always recommended to obtain a maintenance window when making any changes to the server.

Special Instructions for High Availability Systems:

For systems that have High Availability configured via the System Platform Webconsole, you do not need to stop and remove HA.

However, you **MUST** ensure that the system is fully synced prior to proceeding with the scripted installation.

After ensuring the system is fully synced, apply the procedures below to dom0 on both servers, and to cdom on the active server. By applying the script on the active server's cdom, it will get replicated to the standby server's disks, so that if HA is stopped in the future, it will be present on both the active and standby cdoms.

Scripted Installation Procedure

1. Download the Avaya Aura® System Platform Bash Shellshock hot fix (*bash-installer-1.0.bsx)* from PLDS to your PC.
2. Copy the *bash-installer-1.0.bsx* file to the /tmp directory on **both** cdom and dom0 and verify the md5sum. Note that you will need to utilize a tool such as WinSCP to copy the file to cdom and dom0.

   Verify the md5sum.

   For example:

```
[admin@ha1dom0 tmp]# md5sum bash-installer-1.0.bsx
2713d7a839d82bcede4922623f633be3  bash-installer-1.0.bsx
```

3. On dom0, become super user (note that customers own the root login on System Platform cdom and dom0)

```
      [admin@ha1dom0 ~]$ su -
      Using major release number R016x on System Platform
      Password:
      Last login: Fri Oct  3 10:49:51 MDT 2014 from 192.168.1.1 on ssh
      You have logged into dom0 of the System Platform.
      To view a list of installed domains, use the command xm list.
      To reach another domain from here, you can ssh to that domain's
      public IP address or use the xm console command. The xm commands
      (xm list, xm console) require root permission.
      [root@dellha1dom0 ~]#
```

4. Change to the /tmp directory

```
      [root@ha1dom0 ~]# cd /tmp
```

5. Run the self-extracting installer

```
 [root@ha1dom0 tmp]# sh ./bash-installer-1.0.bsx

Self Extracting Installer

./bash-3.2-33.el5_11.4.AV1.x86_64.rpm
./installer
Running bash Installer
Preparing...                ########################################### [100%]
   1:bash                   ########################################### [100%]
```

6. Verify the fix was applied correctly by checking the version of the bash rpm. It should report as **bash-3.2-33.el5_11.4.AV1.x86_64**

```
 [root@ha1dom0 tmp]# rpm -qf /bin/bash
 bash-3.2-33.el5_11.4.AV1.x86_64
```

7. Repeat steps 3-6 for cdom.

Workaround or alternative remediation

N/A.

Remarks

Note:

More information on the change can be found in the **Avaya Security Alert, ASA-2014-369.**
https://downloads.avaya.com/css/P8/documents/100183009

Patch Notes

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

Backup before applying the patch

Download

https://plds.avaya.com. Under System Platform. Download ID SP00000040.

Patch install instructions	Service-interrupting?
Changes applied via scripted installation described above.	No

Verification

Additional verification beyond what was provided above.

If the **vulnerability is present**, execution of the following command will result in the following where the word “vulnerable” is in the output:

```
[root@ha1dom0 ~]# env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

If the **vulnerability has been fixed**, execution of the following command will result in the following where only “this is a test” is displayed in the output, the word “vulnerable” is not printed:

```
[root@ha1dom0 ~]# env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
this is a test
```

Failure

Contact Technical Support.

Patch uninstall instructions

Once activated these changes 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

Vulnerability	**Description**
CVE-2014-6271	bash: specially-crafted environment variables can be used to inject shell commands
CVE-2014-7169	bash: code execution via specially-crafted environment (Incomplete fix for CVE-2014-6271)
CVE-2014-7186	bash: parser can allow out-of-bounds memory access while handling redir_stack
CVE-2014-7187	bash: off-by-one error in deeply nested flow control constructs

Avaya Security Vulnerability Classification

High

Mitigation

Apply scripted installation procedures described above.

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

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.