Product Support Notice

PSN #	PSN004314u			
Original publication date: 16-Oct-14. This is Issue #01, published date: 16-Oct-14.	Severity/risk level	High	Urgency	Immediately
Name of problem	Collaboration Environment (CE) Shellshock bash vulnerability fix			

Products affected

Avaya Aura® Collaboration Environment Release 3.0 and 3.0.1

Problem description

A bash vulnerability known as “shellshock” was recently discovered that affects Collaboration Environment. The Avaya bash shellshock ASA response for Collaboration Environment can be found at https://downloads.avaya.com/css/P8/documents/100183009.

This fix updates the bash rpm to the latest version provided by Red Hat and remediates the vulnerabilities associated with the following CVEs:

- CVE-2014-7169 bash: code execution via specially-crafted environment (Incomplete fix for CVE-2014-6271)
- CVE-2014-6271 bash: specially-crafted environment variables can be used to inject shell commands
- CVE-2014-7186 bash: denial of service due to redirect implementation out-of-bounds
- CVE-2014-7187 bash: off-by-one error in deeply nested flow control constructs

This fix also remediates breakage in the Red Hat “at” package:

- RHBA-2014:1362-1 at: Due to a security issue fix in Bash, "at" jobs failed to run because the "atd" daemon exported environment variables with an incorrect syntax to the Bash shell running the jobs.

Resolution

This fix is designed to be installed on the following service packages/platforms:

CE 3.0

CE 3.0.1

Workaround or alternative remediation

None

Remarks

This patch is applicable to the CE 3.0 and the CE 3.0.1 releases. Future releases (CE 3.0.2 and later) will have this fix included in the base load and will not need this patch. Inquiries about patches for previous versions of CE (CE 2.0) should be made through a customer support ticket via the Avaya Support Webpage.

Patch Notes

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

Backup before applying the patch

This patch is service affecting, and CE should be placed in a Deny New Service state before installing the patch.

Download

Download the CE 3.0 Shellshock bash Patch (filename **ce-patch-rhel-6.2.0-sp2.bin**) from PLDS via ID CE000000040: CE 3.0 Shellshock bash Patch.

Patch install instructions	Service-interrupting?
Copy the patch file (**ce-patch-rhel-6.2.0-sp2.bin**) to a directory such as your home directory (/home/<user>). The patch should have the following Linux permissions: “rw-r--r–“	Yes

Once downloaded, verify the md5sum with:

```
$ md5sum /home/<user>/ce-patch-rhel-6.2.0-sp2.bin
```

```
8c0433392002943271acf7c7fa87e4e8
```

If the MD5 checksum matches above, then the patch should be installed using the following procedure:

1) Place the CE server into a Deny New Service state from the System Manager > Elements > Collaboration Environment > Server Administration screen.
2) Log into the Collaboration Environment shell as the craft or customer user
3) Install the patch by executing the patchCE command and passing it the filename of the patch:
    - `$ patchCE /home/cust/ce-patch-rhel-6.2.0-sp2.bin`

You will see a warning message that the patch is service interrupting and will prompt you to continue. If so, answer “Yes” and the patch will install.

4) Once installed, the fix is active and a reboot is not required. Now place the CE server into an Accept New Service state from the System Manager > Elements > Collaboration Environment > Server Administration screen.

Verification

After installation completes, run the following command:

```
$ cat /opt/Avaya/install.properties
```

The last line of the output should display:

```
securityUpdateVersion=rhel-6.2.0-sp2
```

This patch updates the Linux bash rpm, so another way to verify that the fix has been applied is to run this command:

```
$ rpm –q bash
```

The output should read:

```
bash-4.1.2-15.el6.2.AV1.x86_64
```

Failure

If the installation of the patch fails, retry the installation. If problems persist, contact Avaya Support.

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

Risks associated with not applying this patch are detailed in each of the relative CVE’s listed below:

- CVE-2014-7169 bash: code execution via specially-crafted environment (Incomplete fix for CVE-2014-6271)
- CVE-2014-6271 bash: specially-crafted environment variables can be used to inject shell commands
- CVE-2014-7186 bash: denial of service due to redirect implementation out-of-bounds
- CVE-2014-7187 bash: off-by-one error in deeply nested flow control constructs

Avaya Security Vulnerability Classification

High

Mitigation

Apply the patch referenced herein to all CE 3.0 or 3.0.1 servers. For earlier CE versions, contact Avaya Support.

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.