Product Support Notice

PSN #	PSN004344u

Original publication date: 24-Oct-14. This is Issue #01, published date: 24-Oct-14.

Severity/risk level	High	Urgency	Now

Name of problem ShellShock Linux Bash vulnerability on CES

Products affected

Avaya one-X Client Enablement Services Release 6.2.2 & 6.2.3

Problem description

Possible vulnerability to security attacks for customers who have installed Avaya Client Enablement Services 6.2.2 or 6.2.3 on System Platform, this issue will be addressed by the patch released with this PSN. For customers who have installed directly on Linux, the customer should refer to their Linux vendor's instructions for resolving this issue.

No solution is planned for customers running older version of the CES (e.g. 6.1.x) , and they are encouraged to upgrade to 6.2.3.

Resolution

Apply the patch provided on Avaya support site: https://support.avaya.com/downloads/download-details.action?contentId=C2014721156525200_4&productId=P0984&releaseId=6.2.x

file name: `patchCES.bin`

Patch Notes

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

Backup before applying the patch

Follow the instruction provided in the readme file included with the patch

Download

```
- scp the patchCES.bin on to the one-X CES Server using craft user.
- ssh to the one-X CES Server using craft user and switch to root.
```

Patch install instructions — **Service-interrupting?** Yes- Reboot required

```
Steps for the installation of the patchCES.bin
- Run the patchCES.bin as root user.
        output:
        [root@cesdev212 tmp]# ./patchCES.bin
```

More details included in the read me file, please make sure to follow

Verification

```
Verifying archive integrity... All good.
        Uncompressing one-X CES Patch...
        Extraction finished successfully.
        Checking one-X CES version...
      one-X CES Version 6.2.3 found...
```

Failure

NA

Patch uninstall instructions

NA

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.