Product Support Notice

PSN #	PSN004306u

Original publication date: 6-Oct-14. This is Issue #01, published date: 6-Oct-14.

Severity/risk level	High	Urgency	When convenient

Name of problem AS 5300 Bash Shellshock hotfix

Products affected

Avaya Aura® Application Server 5300 (AS 5300) Release: 2.0 and 3.0

Problem description

This hotfix is for the bash vulnerability known as “shellshock”.

This hotfix updates bash to the latest version provided by RedHat 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: 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

The version of bash after running this hotfix is bash-3.2-33.el5_11.4.

Resolution

This hotfix has been tested on the following service packages/platforms:

- R2.0 PB28 (platform version 13.0.36)
- R3.0 App Bundle (platform version 15.0.17)
- R3.0 SP7 (platform version 15.0.40)
- R3.0 SP8 (platform version 15.0.42)
- R3.0 SP8 EMR (platform version 15.0.43)
- R3.0 SP9 (platform version 15.0.44)

Any AS 5300 system running a service package that is NOT mentioned in the above list is urged to upgrade to one of the listed service packages before applying this hotfix.

Workaround or alternative remediation

n/a

Remarks

This hotfix is different than the normal platform patch in that it only updates the bash package on the system. The platform version number will **not** change after applying this hotfix.

Patch Notes

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

Backup before applying the patch

n/a

Download

Download the hotfix “Application Server 5300 Bash Shellshock Hotfix” (filename **shellshock.tar**) from the Avaya Support Portal on the AS 5300 R3.0 Support Downloads page.

Even though this hotfix is located in the R3 section of the AS 5300 support portal, the same hotfix file applies to both AS 5300 R2 and AS 5300 R3.

Patch install instructions

Service-interrupting?

Perform the following steps on **EVERY** SIP Core and AMS/MAS server in the AS 5300 system: No

1. Transfer the file shellshock.tar to /var/mcp/media as an SSA user
2. SSH to the server as an SSA user
3. Execute the following commands:
    a. su - (enter root password when prompted)
    b. cd /var/mcp/media
    c. tar –xvf shellshock.tar
    d. ./bashdoor_HotFix.sh
        i. Press Y when asked to install bash
4. Verify that the output from the bashdoor_HotFix.sh matches the following:

    ### [100%]
    ### [100%]
    The bash-3.2-33.el5_11.4.x86_64.rpm was installed.
    File permissions update OK.
    Current bash version is 'bash-3.2-33.el5_11.4'

The bash upgrade is applied immediately and a reboot is not required after running the hotfix.

IMPORTANT: **EVERY** SIP Core and AMS/MAS server in the AS 5300 system **MUST** have this hotfix manually applied via the above steps to remediate the bash vulnerability on each server.

Verification

Once the patch has been applied, perform the following command:

- `rpm -q bash`

The output from this command will show the version number of the updated bash package, which should be bash-3.2-33.el5_11.4.

Bash can also be manually tested by running the following command from the command line:

```
env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c "echo test"
```

The **vulnerable** bash versions will print out the following:

```
vulnerable
bash: BASH_FUNC_x(): line 0: syntax error near unexpected token `)'
bash: BASH_FUNC_x(): line 0: `BASH_FUNC_x() () { :;}; echo vulnerable'
bash: error importing function definition for `BASH_FUNC_x'
test
```

The **NON** vulnerable bash version will print out the following:

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `BASH_FUNC_x'
test
```

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

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.