Product Support Notice

PSN #	PSN027009u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 23-Oct-14. This is Issue #2, published date: 28-Oct-14.

Severity/risk level	High	Urgency	Immediately

Name of problem PSN027009u – Avaya Aura® Utility Services update for the Bash shell vulnerability (Shellshock)

Products affected

Avaya Aura® Utility Services 6.1.x, 6.2.x, 6.3.x
Avaya Aura® Communication Manager (CM), Release 6.2, 6.3
Avaya Aura® Solution for Midsize Enterprise, Release 6.2, 6.2.2
Avaya Aura® System Platform, Release 6.2.x, 6.3.x
S8300 Server
S8800 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

Resolution

Utility Services Patch 6.1.1.2.8 is available for any 6.1.x Utility Services Virtual Machine.
Utility Services Patch 6.2.0.3.15 is available for any 6.2.x Utility Services Virtual Machine.
Utility Services Service Pack 6.3.6.0.20 will be available for any 6.3.x Utility Services Virtual Machine on Oct 20.

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.
Patch 6.1.1.2.8 – PLDS Download ID: CM000000207
Patch 6.2.0.3.15 -- PLDS Download ID: US000000040
Service Pack 6.3.6.0.20 -- PLDS Download ID: US000000039

Patch install instructions	Service-interrupting?
Use System Platform's standard patching interface via the CDOM Webconsole for an installed template. It is always recommended to obtain a maintenance window when making any changes to the server.	Yes

Utility Services 6.1.x:

Patch 6.1.1.2.8 can be applied to ANY 6.1.x Utility Services Virtual Machine, regardless of other patches installed. You should NOT remove any existing patches or service packs. This is **NOT service affecting.**

Utility Services 6.2.x:

Patch 6.2.0.3.15 can be applied to ANY 6.2.x Utility Services Virtual Machine, regardless of other patches installed. You should NOT remove any existing patches or service packs. This is **NOT service**

affecting.

Utility Services 6.3.x:

Service Pack 6.3.6.0.20 is a cumulative service pack and contains all fixes provided in previous service packs. Please follow standard Utility Services patch application procedures where the existing service pack should first be removed before applying the latest service pack. This **IS service affecting**.

Please see PSN027002u if the system is currently on either 6.3.1.0.20 or 6.3.2.0.20 and apply those procedures first.

Verification

For both 6.2.x and 6.3.x, 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.

```
[admin@localhost ~]$ rpm –qa |grep bash
bash-3.2-33.el5_11.4
```

Optional Verification Steps:

If the vulnerability is present:

Test 1:

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

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

Test 2:

If the **vulnerability is present**, execution of the following command will result in the following where bash errors and the current date are displayed in the output. Note below the current date of "Thu Oct 23 18:07:54 MDT 2014" is printed.

```
[admin@localhost ~]$ env X='() { (shellshocker.net); cat echo; rm ./echote"
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
Thu Oct 23 18:07:54 MDT 2014
```

If the vulnerability has been fixed:

Test 1:

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:

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

Test 2:

If the **vulnerability has been fixed**, execution of the following command will result in the following where only the word "date" & the specific cat and rm errors are displayed in the output. The actual current date is not printed:

```
[admin@localhost ~]# env X='() { (shellshocker.net)=>\' bash -c "echo date"; cat echo; rm ./echo
      date
      cat: echo: No such file or directory
      rm: cannot remove `./echo': No such file or directory
```

Failure

Contact Technical Support.

Patch uninstall instructions

Once activated, this change cannot be removed, even if the service pack or patch is 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 patches noted 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