Product Support Notice

PSN #	PSN027008u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 10-Oct-14. This is Issue #1, published date: 10-Oct-14.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN027008u –Avaya Virtual Application Manager update for the Bash shell vulnerability (Shellshock)				

Products affected

Avaya Virtual Application Manager 6.2.x

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

AVAM-Patch-06.02.00.2227.tar.gz updates the AVAM Linux Bash shell to address the Shellshock vulnerability. This patch is applicable for all builds of AVAM up to and including the GA build, AVAM-6.2.0.2226-e50-78.ova.

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

Perform a backup of AVAM before applying the patch.

Download

https://plds.avaya.com. Under Application Communication Manager . PLDS Download ID AVAM0000002.
AVAM-Patch-06.02.00.2227.tar.gz

Patch install instructions	Service-interrupting?
Follow the normal AVAM patching procedure to upload and apply the patch. Refer to the document: Administering the Avaya Virtual Application Manager. https://downloads.avaya.com/css/P8/documents/100179598	No

Verification

Verify the fix was applied correctly by checking the version of the bash rpm. It should report as **bash-4.1.2-15.el6_5.2.x86_64**

```
[admin@localhost ~]$ rpm -qf /bin/bash
bash-4.1.2-15.el6_5.2.x86_64
```

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
```

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
```

Failure

Contact Technical Support.

Patch uninstall instructions

Once activated, this change cannot be removed. Although the "Rollback Patch" option is available in the AVAM patching administration screen once the patch has been installed, the script that this invokes will NOT remove the patch rpm.

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