Product Support Notice

PSN #	PSN020149u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 8-Oct-14. This is Issue #4, published date: 21-Sep-15.	Severity/risk level	High	Urgency	Immediately

Name of problem	Communication Manager updates for the Bash shell vulnerability (Shellshock).

Products affected

Avaya Aura® Communication Manager (CM), Releases 5.0 - 6.3
Avaya Aura® Solution for Midsize Enterprise, Releases 6.x.x
S8300 Server
S8400 Server
S8500 Series Servers
S8700 Series Servers
S8800 Server
Common Servers (HP & Dell)

Problem description

This problem occurs in Avaya Aura® Communication Manager (CM) Releases 5.0 – 6.3

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. 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.
ASA-2014-369

Resolution

This problem is fixed in CM 5.2.1 hot over-writable Bash Shellshock patch 21907.
Over-writable Bash Shellshock Patch 21907

This problem is fixed in CM 6.0.1 hot over-writable Bash Shellshock patch 21906.
Over-writable Bash Shellshock Patch 21906

This problem is fixed in CM 6.2 hot over-writable Bash Shellshock patch 21905.
Over-writable Bash Shellshock Patch 21905

This problem is fixed in CM 6.3 hot over-writable Bash Shellshock patch 21904. This patch applies only to CM 6.3.xx.x and not CM 6.3.1xx.x.
Over-writable Bash Shellshock Patch 21904

This problem is fixed in CM 6.3 Security Service Pack (SSP) 6 and higher CM 6.3 SSPs. CM SSP 6 and higher SSPs apply to both CM 6.3 loads R016x.03.0.124.0 (CM 6.3.xx.x) and R016x.03.0.141.0 (CM 6.3.1xx.x). For CM 6.3.1xx.x SSP 6 and higher must be used and an over-writable patch is not available.
CM 6.3 SSP 6

This problem is fixed in CM 7.0 and later Releases.

The patch download links are located at the bottom of the linked support pages referenced above.

NOTE: All CM releases earlier/lower than CM 5.2.1, including earlier CM 5.x.x. releases, will not have patches available for remediation. These earlier CM releases are End of Manufacturer Support (EOMS).

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

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

Backup before applying the patch

Always

Download

Use the links provided in the Resolution section of this document to download the respective patches.

Patch install instructions

Service-interrupting?

No

These patches are customer installable and remotely installable.

These patches are hot patches (non-service affecting) and over-writable (designed to be activated on top of currently activated CM patches/SPs). However, it is recommended that the patches be activated during a maintenance window using the same instructions provided in the “Finding the installation instructions” sections of the Service Pack PCNs for each respective CM release:

PCN1921S or PCN1798S should be used for CM 6.3.

PCN1792S should be used for CM 6.2.

PCN1720S should be used for CM 6.0.1.

PCN1691S should be used for CM 5.2.1.

Do not deactivate any existing CM patches or service packs running on the system before activating the over-writable patches. Over-writable patches are designed to be activated on top of currently activated CM patches/SPs.

Note that for CM 6.3 Security Service Pack 6 can be used instead of the over-writable CM 6.3 patch, and must be used for CM 6.3 load R016x.03.0.141.0 (6.3.1xx.x).

Note that these over-writable patches are not dependent on any specific version of Service Pack, KSP or SSP. They can be activated over any SP, KSP or SSP currently running on the system. No Service Pack, KSP or SSP upgrade is required. The exception to this is that SSP 6 or higher can be used to remediate CM 6.3 releases.

Verification

Patch installation instructions include verification instructions.

Failure

Contact Technical Support.

Patch uninstall instructions

Once activated these patches cannot be deactivated (uninstalled). The deactivate step will succeed, but the updated bash rpm will not be 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 hot over-writable patches described above.

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.