Product Support Notice

PSN #	PSN004438u

Original publication date: 09-Mar-15. This is Issue #01, published date: 09-Mar-15.

Severity/risk level	Medium	Urgency	Immediately

Name of problem Session Manager GHOST glibc vulnerability fix

Products affected

Avaya Aura® Session Manager: Release 1.1 through 6.3.12

Problem description

The Ghost glibc vulnerabilities were recently discovered which affect Session Manager. The Avaya GHOST ASA responses for Session Manager can be found at https://downloads.avaya.com/css/P8/documents/101006704/

This PSN details a patch for the Session Manager to address these vulnerabilities associated with the following CVEs:

- CVE-2015-0235 glibc: __nss_hostname_digits_dots() heap-based buffer overflow

Resolution

A patch was developed that can be installed on all releases of Session Manager from 6.2.0 through 6.3.12. Releases prior to 6.2 will not be patched for this issue, and should be upgraded to a newer release of Session Manager with the required patch detailed in this PSN. Once applied, future service pack installs will detect if these glibc rpm's are newer, and if so will leave them in place, and the patch will not need to be re-applied. The patch will also be included as part of the 6.3.13 and later Session Manager software releases.

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

This patch is service affecting, and the Session Manager should be placed in a Deny New Service state before installing the patch.

Download

The patch file can be downloaded from PLDS via download ID SM000000077: Session Manager GHOST Patch for 6.2 through 6.3.12

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

Download the patch and copy it to the Session Manager server in a binary mode. WinSCP can be used to copy the file and is available on the internet for download. Once the patch has been copied to the Session Manager server, verify it's MD5 Checksum matches:

$ md5sum /home/cust/asm-patch-ghost.bin
4c91c9476d18811f446ca4aa35e2db42

If the MD5 checksum matches above, then the patch should be installed using the following procedures:

1) Place the Session Manager server into a Deny New Service state from the System Manager > Elements > Session Manager > Dashboard screen.
2) Log into the Session Manager as the craft or customer user
3) Install the patch by executing the patchSM command and passing it the filename of the patch:
   - $ patchSM /home/cust/asm-patch-ghost.bin

   NOTE: The patch installation will result in a reboot of the Session Manager server.
4) After the Session Manager reboots, place the Session Manager server into an Accept New Service state from the System Manager > Elements > Session Manager > Dashboard screen.

Verification

NOTE: The ***swversion*** command, and the Element Manager Dashboard display will not show that the ghost patch has been applied. The steps below are the only way to verify that this patch has been applied properly.

You can verify the appropriate patch has been installed on the Session Manager server by ensuring that the bash rpm version matches the appropriate version below via the Red Hat Enterprise Linux ***rpm*** command. It must be run from Session Manager server command line interface via the cust or craft login.

For Session Manager 6.3.X:

$ rpm –q glibc | grep i686
glibc-2.12-1.149**.el6_6.5**.i686

For Session Manager 6.2.X:

$ rpm -q glibc
glibc-2.5-**123**.el5_11.1
glibc-2.5-**123**.el5_11.1

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

Risks associated with not applying this patch are detailed in each of the relative CVE's listed below:

- CVE-2015-0235 glibc: __nss_hostname_digits_dots() heap-based buffer overflow

Avaya Security Vulnerability Classification

Medium

Mitigation

Apply the patch referenced in this PSN to the Session Manager 6.2 through 6.3.12 server. If Session Manager version is prior to 6.2, then an upgrade to a Session Manager 6.3.x release is required before applying the appropriate patch.

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.