



Product Support Notice

© 2014 Avaya Inc. All Rights Reserved.

PSN # PSN004331u

Original publication date: 16-Oct-14, This is issue #04, published date: 09-Dec-14.

Severity/risk level

High

Urgency

Optional

Name of problem Bash shell vulnerability (Shellshock) patch for Avaya Aura® System Manager and WebLM releases

Products affected

Avaya Aura System Manager release 1.0 through 6.3.10

WebLM (VMWare) release 6.2.x, 6.3.0, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.7, 6.3.8 and 6.3.10.

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

This PSN introduces the Bash shell vulnerability (Shellshock) patch for System Manager 6.2.x, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9 and 6.3.10 releases and for WebLM(VMWare) 6.2.x, 6.3.0, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.7, 6.3.8 and 6.3.10 releases.

Applying **SystemManager_WebLM_Shellshock_Patch.bin** patch will fix the above mentioned problems in Avaya Aura® System Manager 6.2.x, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9 and 6.3.10 releases and WebLM(VMWare) Server 6.2.x, 6.3.0, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.7, 6.3.8 and 6.3.10 releases.

Note:

- If the patch is already installed on the 6.2.x release and system is upgraded to 6.3.x release, then install this patch again after upgrade.
- If the patch is already installed on 6.3.x release and system is upgraded to a higher 6.3.x release (from 6.3.1 to 6.3.10), then install this patch again after upgrade.

Workaround or alternative remediation

NA

Remarks

This patch must be applied on:

Avaya Aura® System Manager 6.2.x, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9 and 6.3.10 releases

Or,

WebLM 6.2.x, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.7, 6.3.8 and 6.3.10 releases

Note: In case the Avaya Aura® System Manager release is prior to the above releases, upgrade to 6.3.x first to use this fix.

Follow the below steps to determine which Avaya Aura® System Manager or WebLM release your server is running.

1. Log on to the System Manager/WebLM Web console.
2. Click the “About” link on the home/landing page. Verify that the About page contains as below:
 - For System Manager 6.2.x Release:

Release	Build No
Avaya Aura® System Manager 6.2 GA	6.2.0.0.15669-6.2.12.9 and Software Update Revision No: 6.2.12.1.xxxx
Avaya Aura® System Manager 6.2 Service Pack 1	6.2.0.0.15669-6.2.12.105 and Software Update Revision No: 6.2.13.1.xxxx
Avaya Aura® System Manager 6.2 Service Pack 2	6.2.0.0.15669-6.2.12.202 and Software Update Revision No: 6.2.14.1.xxxx

Avaya Aura® System Manager 6.2 Service Pack 3	.2.0.0.15669-6.2.12.307 and Software Update Revision No: 6.2.15.1.xxxx
Avaya Aura® System Manager 6.2 Service Pack 4	6.2.0.0.15669-6.2.12.408 and Software Update Revision No: 6.2.16.1.xxxx

- For System Manager 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9 and 6.3.10 releases.

Release	Build No
Avaya Aura® System Manager 6.3.0 GA	6.3.0.8.5682-6.3.8.818 and Software Update Revision No: 6.3.0.8.xxxx
Avaya Aura® System Manager 6.3.1	6.3.0.8.5682-6.3.8.859 Software Update Revision No: 6.3.1.9.xxxx
Avaya Aura® System Manager 6.3.2	6.3.0.8.5682-6.3.8.1627 Software Update Revision No: 6.3.2.4.xxxx
Avaya Aura® System Manager 6.3.3	6.3.0.8.5682-6.3.8.1814 Software Update Revision No: 6.3.3.5.xxxx
Avaya Aura® System Manager 6.3.4	6.3.0.8.5682-6.3.8.2631 Software Update Revision No: 6.3.4.4.xxxx
Avaya Aura® System Manager 6.3.5	6.3.0.8.5682-6.3.8.2807 Software Update Revision No: 6.3.5.5.xxxx
Avaya Aura® System Manager 6.3.6	6.3.0.8.5682-6.3.8.3007 Software Update Revision No: 6.3.6.6.xxxx
Avaya Aura® System Manager 6.3.7	6.3.0.8.5682-6.3.8.3204 Software Update Revision No: 6.3.7.7.xxxx
Avaya Aura® System Manager 6.3.8	6.3.0.8.5682-6.3.8.4219 Software Update Revision No: 6.3.8.5.xxxx
Avaya Aura® System Manager 6.3.9	6.3.0.8.5682-6.3.8.4414 Software Update Revision No: 6.3.9.1.xxxx
Avaya Aura® System Manager 6.3.10	6.3.0.8.5682-6.3.10.7.2656 Software Update Revision No: 6.3.10.7. xxxx

- For WebLM 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.7, 6.3.8 and 6.3.10 releases.

Release	Build No
WebLM 6.3.2	Web License Manager (WebLM v6.3) Build Number - 6.3.2.X.XXXX
WebLM 6.3.3	Web License Manager (WebLM v6.3) Build Number - 6.3.3.X.XXXX
WebLM 6.3.4	Web License Manager (WebLM v6.3) Build Number - 6.3.4.X.XXXX
WebLM 6.3.5	Web License Manager (WebLM v6.3) Build Number - 6.3.5.X.XXXX
WebLM 6.3.7	Web License Manager (WebLM v6.3) Build Number - 6.3.7.X.XXXX
WebLM 6.3.8	Web License Manager (WebLM v6.3) Build Number - 6.3.8.X.XXXX
WebLM 6.3.10	Web License Manager (WebLM v6.3) Build Number - 6.3.10.X.XXXX

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

Follow the instructions below to download the patch:

1. Go to <http://support.avaya.com>
2. Click on “Downloads & Documents” link on the dashboard menu.
3. Enter product name as “System Manager” and then select “Avaya Aura® System Manager”
4. Select the version corresponding to your System Manager installation (6.2.x or 6.3.x) from the dropdown.
5. Click on the appropriate download link as per your System Manager Installation version. E.g.: Click “System Manager and WebLM Shellshock Patch” if you have System Manager Release 6.2 installed.
6. Go to the “Downloads” tab and click on the link to the file “SystemManager_WebLM_Shellshock_Patch.bin” to download the utility.
7. Use download id “**SMGRSHPC01**” to download the path from PLDS.

Patch install instructions

Service-interrupting?

IMPORTANT: If System Manager installation is a Geo-Redundancy enabled deployment, Geo-Redundancy should be disabled, the patch should be applied to both Primary and Secondary System Manager systems, and then re-enable Geo-Redundancy.

No

Follow the instructions below to install the patch:

1. Download the patch file (SystemManager_WebLM_Shellshock_Patch.bin) from support site (<http://support.avaya.com>).
2. Copy (SystemManager_WebLM_Shellshock_Patch.bin) into the /tmp/ directory of the System Manager.
3. Get access to the System Manager Command Line Interface using appropriate local OS user with root level permission.
4. Execute the patch file using the following command on the System Manager server :
cd /tmp/
chmod +x SystemManager_WebLM_Shellshock_Patch.bin
sh SystemManager_WebLM_Shellshock_Patch.bin

Verification

Execute the following commands from CLI, before & after applying the hotfix –

```
# env x=() { ;;}; echo vulnerable' bash -c "echo this is a test"
```

- Before applying this patch following is the command output –
vulnerable
this is a test

- After applying the hotfix, following is the command output –
this is a test

```
# cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>' bash -c "echo date"; cat /tmp/echo
```

- Before applying this patch following is the command output –
bash: x: line 1: syntax error near unexpected token `='
bash: x: line 1: `
bash: error importing function definition for `x'
Thu Oct 16 18:30:09 MSK 2014

Note: A file called **/tmp/echo** will be created.

- After applying the hotfix, following is the command output –

date

cat: /tmp/echo: No such file or directory

Note: No file will be created .

Failure

In case of issues with the patch installation, Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs along the failure logs at location /var/log/Avaya/BashShellShockFix.log

Patch rollback 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](#).

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.