



Product Support Notice

© 2014 Avaya Inc. All Rights Reserved.

PSN # PSN004350u

Original publication date: 29- Oct-14. This is Issue #02, published date: 29- Oct-14.

Severity/risk level

High

Urgency

Immediately

Name of problem 0040 – Meeting Exchange update for the Bash shell vulnerability (Shellshock)

Products affected

Meeting Exchange 5.2.X, 6.2.X

Avaya Aura Conferencing 6.0.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

Meeting Exchange 5.2.X: Only the MX Bridge needs to be updated for the Bash shellshock fix. Please download the bash-3.0-27.el4.4.i386.rpm (Bash shell vulnerability (Shellshock) update).

This self-extracting executable script is posted on PLDS under Conferencing, PLDS Download ID MX000000214.

Meeting Exchange 6.2.X & AAC 6.0.X:

For CRS, WP & AWC, patch the system Platform by referring to PSN at <https://downloads.avaya.com/css/P8/documents/100183127>

For MX Bridge & Web Portal: You will need to download the bash-3.2-33.el5_11.4.i386.rpm (Bash shell vulnerability (Shellshock) update).

This self-extracting executable script is posted on PLDS under Conferencing, PLDS Download ID MX000000213.

The following procedure should be applied to

- MX bridge 5.2.X
- MX Bridge & WebPortal 6.2.X
- AAC Bridge & WebPortal 6.0.X

While this procedure is not service affecting, it is always recommended to obtain a maintenance window when making any changes to the server.

1. Copy the rpm to the vulnerable machine under /tmp/ directory using WinScp.
2. Verify the md5sum of the copied file:

For MX 5.2.X

*md5sum bash-3.0-27.el4.4.i386.rpm
it should match to 64cb32f853b208a36335208e3b2ccc61*

For MX Bridge 6.2.X, WebPortal 6.2.X, AAC Bridge 6.0.X & AAC Web Portal 6.0.X

*md5sum bash-3.2-33.el5_11.4.i386.rpm
it should match to e579bd3f1fe173393483db540ec1ab13*

3. Become super user (sroot) (*su – sroot*)
4. Install the rpm with the command below:

For MX 5.2.X

```
rpm -Uvh --nodeps bash-3.0-27.el4.4.i386.rpm
```

For MX Bridge 6.2.X, WebPortal 6.2.X, AAC Bridge 6.0.X & AAC Web Portal 6.0.X

```
rpm -Uvh --nodeps bash-3.2-33.el5_11.4.i386.rpm
```

5. 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.AV1.x86_64 for MX 6.2 & AAC 6.0
It should report as bash-3.0-27.el4.4.XXX for MX 5.2

```
[sroot@bridge1 tmp]# rpm -qf /bin/bash  
bash-3.2-33.el5_11.4.AV1.x86_64
```

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> Under Conferencing. Download ID MX000000214 (for MX 5.2)

<https://plds.avaya.com> Under Conferencing. Download ID MX000000213 (for MX 6.2 & AAC 6.0)

Patch install instructions

Service-interrupting?

Changes applied via scripted installation described above

No

Verification

Additional verification beyond what was provided above.

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

```
env 'x=() { :}; echo vulnerable' 'BASH_FUNC_x()=() { :}; echo vulnerable' bash -c "echo test"
```

```
vulnerable
```

```
bash: BASH_FUNC_x(): line 0: syntax error near unexpected token `)'
```

```
bash: BASH_FUNC_x(): line 0: `BASH_FUNC_x() () { :}; echo vulnerable'
```

```
bash: error importing function definition for `BASH_FUNC_x'
```

```
test
```

If the vulnerability has been fixed, execution of the same command will result in the following where the word “vulnerable” is not printed:

Failure

Contact Technical Support

Patch uninstall instructions

Once activated these changes should 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 scripted installation procedures 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](#).

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.