Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN #	PSN004216u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 24-Mar-2015. This is Issue #01, published date: 24-Mar-2015.

Severity/risk level	Low	Urgency	When convenient

Name of problem CMS mitigation for "Freak" SSL vulnerability

Products affected

All R16.3 and R17 CMS Servers on all platforms

Problem description

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role.

To minimize the risk customers should:

- move to the latest R17 (r17jb.a) or R16.3 (r16.3fa.b) load.

AND

- Update the Linux RPMs
- Update the Solaris patch

Resolution

Operating System patches and rpms will be incorporated into the next product releases for CMS R16.3 and CMS R17

Workaround or alternative remediation

This workaround is customer installable. Customers may also contact their Avaya support organization or business partner regarding the installation of this patch. Installation by Avaya *is billable at current per incident rates.* This workaround can be installed following the instructions below:

Step 1 – Install Linux security rpms (if applicable)

a) Move to the latest R17 (r17jb.a) CMS load. If this is not done, required dependent rpms could be missing.

b) Download the following files to /tmp on the CMS system.

File	Download from
openssl-1.0.1e-30.el6_6.7.i686.rpm	https://support.avaya.com/downloads/download-details.action?contentId=C201532412193430_0&productId=P0030&releaseId=17.0.x
openssl-1.0.1e-30.el6_6.7.x86_64.rpm	
openssl-devel-1.0.1e-30.el6_6.7.i686.rpm	

c) Verify the md5sum of the downloaded files.

```
Prompt> cd /tmp
Prompt> md5sum openssl*
      920fca8691266205039e5ef45433fe0f  openssl-1.0.1e-30.el6_6.7.i686.rpm
      3c2fb725d1de94b0b4b503b10c35d04e  openssl-1.0.1e-30.el6_6.7.x86_64.rpm
      ac070b4a60198a918a8bfd595f7940de  openssl-devel-1.0.1e-30.el6_6.7.i686.rpm
```

d) Install the rpms

```
Prompt> rpm -Uvh openssl-devel-1.0.1e-30.el6_6.7.i686.rpm openssl-1.0.1e-
30.el6_6.7.x86_64.rpm openssl-1.0.1e-30.el6_6.7.i686.rpm

Preparing...                ########################################### [100%]
1:openssl                   ########################################### [ 33%]
2:openssl                   ########################################### [ 67%]
3:openssl-devel             ########################################### [100%]
```

e) A reboot is recommended, but not required.

Step 4 - Install Solaris sparc security patches

a) Move to the latest R17 (r17jb.a) or R16.3 (r16.3fa.b) load. This is recommended to get many other Solaris patches for existing security alerts.

b) Download the following files to /tmp on the CMS system. Note: The R16.3 and R17.0 downloads are the same and are accessible from the R17 URLs.

File	Download from
148071-16.zip	https://support.avaya.com/downloads/download-details.action?contentId=C201532412193430_0&productId=P0030&releaseId=17.0.x

c) Verify the md5sum of the downloaded files.

```
Prompt> cd /tmp
Prompt> digest –a md5  148071-16.zip
       (148071-16.zip) = 5add4650402043069bf2e5771b8319dc
```

d) Install the patches

```
Prompt> unzip 148071-16
Prompt> patchadd 148071-16
```

e) A reboot is required for the patch updates to take effect.

Step 5 - Install Solaris x86 security patches

f) Move to the latest R17 (r17jb.a) or R16.3 (r16.3fa.b) load. This is recommended to get many other Solaris patches for existing security alerts.

a) Download the following files to /tmp on the CMS system. Note: The R16.3 and R17.0 downloads are the same and are accessible from the R17 URLs.

File	Download from
148072-16.zip	https://support.avaya.com/downloads/download-details.action?contentId=C201532412193430_0&productId=P0030&releaseId=17.0.x

b) Verify the md5sum of the downloaded files.

```
Prompt> cd /tmp
Prompt> digest –a md5  148072-16.zip
(148072-16.zip) = 79062224917e175c382a1d276f8dac6d
```

c) Install the patches

```
Prompt> unzip 148072-16
Prompt> patchadd 148072-16
```

d) A reboot is required for the patch updates to take effect.

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

yes

Download

openssl-1.0.1e-30.el6_6.7.i686.rpm

openssl-1.0.1e-30.el6_6.7.x86_64.rpm

openssl-devel-1.0.1e-30.el6_6.7.i686.rpm

© 2015 Avaya Inc. All Rights Reserved.

or
148071-16.zip
or
148072-16.zip

Patch install instructions	Service-interrupting?
n/a	Yes

Verification

n/a

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

Avaya Security Vulnerability Classification

Low

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.