Avaya Emerging Products and Technology (EP&T) response to openssl security update (CVE-2014-0160) (Heartbleed Vulnerability)

Original Release Date: April 16th, 2014
Last Revised: April 16th, 2014
Risk Level: None to High
Version: 1.0

1. Overview:

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

An information disclosure flaw was found in the way OpenSSL handled TLS and DTLS Heartbeat Extension packets. A malicious TLS or DTLS client or server could send a specially crafted TLS or DTLS Heartbeat packet to disclose a limited portion of memory per request from a connected client or server. Note that the disclosed portions of memory could potentially include sensitive information such as private keys. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2014-0160 to this issue. Redhat Enterprise Linux specific information may be found in the Redhat CVE Database.

This issue did not affect the versions of openssl as shipped with Red Hat Enterprise Linux 5, and Red Hat Enterprise Linux 6.4 and earlier.

More information about this vulnerability can be found in the security advisories at:

- OpenSSL Security Advisory [07 Apr 2014]
- https://rhn.redhat.com/errata/RHSA-2014-0376.html

2. Avaya EP&T software-only Products:

Avaya EP&T software-only products operate on general-purpose operating systems. Occasionally vulnerabilities may be discovered in the underlying operating system or applications that come with the operating system. These vulnerabilities often do not

impact the software-only product directly but may threaten the integrity of the underlying platform.

In the case of this advisory Avaya software-only products marked with Risk Level 'None' are not affected by the vulnerability directly but the underlying Operating System platform may be. Customers should determine on which operating system the product was installed and then follow that vendor's guidance.

.

Product:	**Versions:**	**Risk Level:**	**Actions:**
Social Media Manager	6.2.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Contact Flow Analytics	7.0	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Avaya Speech Analytics	2.0.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Context Store	1.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Dynamic Self Service (DSS)	2.2	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Dynamic Routing	2.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Callback Assist (CBA)	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.

Avaya Customer Connections Controls (ACC Controls)	1.x, 2.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Avaya Notification Solution (ANS)	1.x – 2.0	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Ajax Toolbar custom solutions	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Ajax Toolbar API	2.1.x	High	Do not configure / activate SSL communication with version 2.1.x until new version is released with correction.

Recommended Actions for EP&T Software-only Solutions Products:
In the event that the affected package is installed, Avaya recommends following recommended actions supplied by the Operating System provider

Mitigating Factors:

When determining risk, Avaya takes into account many factors as outlined by Avaya's Security Vulnerability Classification Policy. The following table describes factors that mitigate the risk of specific vulnerabilities for affected Avaya services products:

Vulnerability	Mitigating Factors
CVE-2014-0160	Disable SSL communication with Ajax Toolbar API 2.1.x until new version is released with correction. There is no risk for the other listed products as the affected openssl version is not installed with the application.

3. Additional Information:

Additional information may also be available via the Avaya support website and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

4. Disclaimer:

ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO 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, INCIDENTAL, STATUTORY, 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.

5. Revision History:

V 1.0 - April 16th, 2014 - Initial Statement issued.
Avaya customers or Business Partners should report any security issues found with Avaya products via the standard support process.
Independent security researchers can contact Avaya at securityalerts@avaya.com.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

© 2014 Avaya Inc. All Rights Reserved. All trademarks identifying Avaya products by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.