Avaya Services Products Response to openssl security update (CVE-2014-0160) (Heartbleed Vulnerability)

Original Release Date: April 11, 2014
Last Revised: May 22, 2014
Risk Level: None to Low
Version: 1.4a
Status: Final

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 Services Solutions Products:

Avaya service solutions are software-only products that can be deployed as standalone applications, or as part of an OVA (VMware virtual machine file), or embedded in the System Platform. They operate on general-purpose operating systems. In some cases openssl is bundled and installed with the application. 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 services solutions are not affected by the vulnerability except for Provision. Customers should determine on which Linux operating system the product was installed and then follow that OS vendor's guidance.

Product:	**Versions:**	**Risk Level:**	**Actions:**
Secure Access Link (SAL) GW	1.x, 2.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Avaya Diagnostic Server (ADS)	1.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Secure Access Remote Access Concentrator	5.x, 6.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Secure Access Core Concentrator	5.x, 6.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Secure Access Link GAS	5.x, 6.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Secure Access Link Policy Server	1.5	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Services VM	1.x, 2.x	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
SAL GW virtual app	1.x (SAL 2.2)	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
ADS virtual app	2.x	None	Depending on the Operating System installed, the affected package may be

			installed on the underlying Operating System.
ProVision	2013.2 and 2013.3 (Earlier affected 2012 versions are no longer usable.)	Low	See Mitigating Factors.
ExpertNet™	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
EXPERT ™	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Avaya Diagnostic Portal Applications™	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
Connect	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
ACSBI	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
OIS	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
SC_SOCKS	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.
SSG	All	None	Depending on the Operating System

			installed, the affected package may be installed on the underlying Operating System.
MSQT	All	None	Depending on the Operating System installed, the affected package may be installed on the underlying Operating System.

Recommended Actions for Services Solutions Products:
In the event that the affected package is installed, Avaya recommends following recommended actions supplied by Red Hat regarding their Enterprise Linux. In the case of OVA deployments, follow CentOS recommendations for the appropriate version of the OS.

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	ProVision may optionally use ssl to support devices. Since ProVision is a client application, the risk is low that a rogue device could be used to explore a limited piece of the ProVision process memory. Notifications sent for further guidance and ProVision 2014.1 release is available now. There is no risk for 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:

V1.0 – April 9, 2014 Initial statement issued.

V1.1 – April 11, 2014 Added additional apps.

V1.2 – April 17, 2014 Downgraded Provision risk to Low. Added clarification on Provision versions affected.

V1.3 – May 7, 2014 EVAT renamed to ExpertNet to be more descriptive. Added Avaya Diagnostic Portal app's.

V1.4 – May 20, 2014 Changed status to Final, notifications sent.

V1.4a – May 22, 2014. Includes ProVision release number.

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.