openssl security update - (RHSA-2005-476)

Advisory Original Release Date: August 29, 2005
Last Revised: August 29, 2005
Number: ASA-2005-170
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

Overview:

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

Multiple security vulnerabilities were discovered in OpenSSL. The first vulnerability could allow a malicious local user to gain portions of cryptographic keys by performing a cache timing attack on certain HyperThreading processors. Avaya products do not operate on HyperThreaded processors and therefore are not affected by this vulnerability.

The second vulnerability could allow a malicious local user to overwrite arbitrary files using the der_chop script. Although Avaya products do not utilize the der_chop script, sertain Avaya products ship with the script installed and therefore are affected by this vulnerability.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2004-0975 and CAN-2005-0109 to these issues.

More information about this vulnerability can be found in the security advisories issued by Red Hat

- https://rhn.redhat.com/errata/RHSA-2005-476.html

Avaya System Products with OpenSSL installed:

Product	Affected S/W Version	Comments and Actions
Avaya™ S8710/S8700/S8500/S8300	All versions	Avaya media servers to do not operate on HypterThreading processors and therefore are only affected by CAN-2005-0109. An update is being considered for a future Major version.
Avaya™ Converged Communication Server	All versions	Avaya media servers to do not operate on HypterThreading processors and therefore are only affected by CAN-2005-0109. An update is being considered for a future Major version.
Avaya™ Intuity LX	Versions	No Action Required. HyperThreading

	1.1-5.x	processors and the der_chop script are not installed.
Avaya™ Modular Messaging – Message Storage Server (MSS)	Version 1.x-2.0	No Action Required. HyperThreading processors and the der_chop script are not installed.
Avaya™ MN100	All versions	No Action Required. HyperThreading processors and the der_chop script are not installed.

Recommended Actions for affected products:

The der_chop script is not part of normal operating procedure of Avaya systems and therefore should not be utilized.

Avaya Software-Only Products

Avaya 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. This vulnerability 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 are not affected by the vulnerability directly but the underlying Linux platform may be. Customers should determine on which Linux operating system the product was installed and then follow that vendors guidance:

Software-Only Products

Product	Affected S/W Version	Actions
Avaya™ CVLAN	All versions	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting CVLAN. Avaya recommends that customers follow the recommended actions supplied by the Operating System vendor (e.g. Red Hat).
Avaya Integrated Management (AIM)	All Versions	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the AIM application. Avaya recommends that customers follow the recommended actions supplied by the Operating System vendor (e.g. Red Hat).

Additional Information: Additional information may also be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

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 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.

Revision History:

V 1.0 - August 29, 2005 - Initial statement issued.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.