

## Updated apache and mod\_ssl packages fix security vulnerabilities - (RHSA-2004-600)

**Advisory Original Release Date:** January 14, 2005

**Last Revised:** February 8, 2005

**Number:** ASA-2005-010

**Risk Level:** Low

**Advisory Version:** 1.1

**Advisory Status:** Interim

### Overview:

Multiple security vulnerabilities were discovered in the apache and mod\_ssl packages:

A buffer overflow was discovered in the mod\_include module. This flaw could allow a local user who is authorized to create server-side include (SSI) files to gain the privileges of a httpd child (user 'apache'). The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2004-0940](#) to this issue. Risk: Low.

The mod\_digest module does not properly verify the nonce of a client response by using a AuthNonce secret. This could allow a malicious user who is able to sniff network traffic to conduct a replay attack against a website using Digest protection. Note that mod\_digest implements an older version of the MD5 Digest Authentication specification, which is known not to work with modern browsers. This issue does not affect mod\_auth\_digest. ([CAN-2003-0987](#)). Risk: Low.

An issue has been discovered in the mod\_ssl module when configured to use the "SSLCipherSuite" directive in a directory or location context. If a particular location context has been configured to require a specific set of cipher suites, then a client is able to access that location using any cipher suite allowed by the virtual host configuration. ([CAN-2004-0885](#)). Risk: Low-None.

More information about this vulnerability can be found in the security advisories issued by Red Hat <<https://rhn.redhat.com/errata/RHSA-2004-600.html>>.

### Recommended Actions:

For all system products which use vulnerable versions of Apache, Avaya recommends that customers restrict access to the IP address of the server and, in particular, ports 80 and 443, to only authorized personnel. This restriction should be enforced through the use of firewalls, ACLs, VPNs, and other generally-accepted networking practices until such time as an update becomes available and can be installed.

### Affected System Products:

<b>Product</b>	<b>Affected S/W Version</b>	<b>Actions</b>
Avaya™ MN100	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.
Avaya™ Intuity LX	1.1-5.x	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.
Avaya™ Modular Messaging MSS	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.
Avaya™ S8710/S8700/S8500/S8300	All Versions	No action required. Communication Manager does not use mod_digest, does not allow modification of web pages after install, and does not use the SSLCiphersuite directive in a directory or location context.
Avaya™ Converged Communication Server	All Versions	No action required. Communication Manager does not use mod_digest, does not allow modification of web pages after install, and does not use the SSLCiphersuite directive in a directory or location context.
Avaya Network Routing (ANR)	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.

### **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. 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 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 vendor's guidance:

### **Software-Only Products**

Product	Affected S/W Version	Actions
Avaya™ CVLAN	All versions	The Linux packages described in this advisory may be installed on the Operating System upon which customers installed the CVLAN application. The CVLAN application does not require the use of these packages. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected application.
Avaya™ Integrated Management	All versions	The Linux packages described in this advisory may be installed on the Operating System upon which customers installed Integrated Management. Integrated Management does not require the use of these packages. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) remove the affected application.

**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 1-866-GO-AVAYA, 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 – January 14, 2005 – Initial statement issued.

V 1.1 – February 8, 2005 – Added Avaya Converged Communication Server. Replaced Avaya Communication Manager listing with appropriate server names (S8x00). Changed advisory status from Final to Interim pending software update.

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

© 2005 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.