

Updated VIM packages fix security issues – (RHSA-2005-010)

Advisory Original Release Date: January 25, 2005

Last Revised: January 25, 2005

Number: ASA-2005-020

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Final

Overview:

A security vulnerability was discovered in VIM. This vulnerability could allow an attacker the ability to execute arbitrary commands by tricking a local system user into opening a carefully crafted file. This vulnerability requires that local system users enable the modeline and filetype plugins. Although certain Avaya system products ship with vulnerable versions of VIM the modelines and filetype plugins are not enabled by default. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2004-1138](#) to this issue.

More information about these vulnerabilities can be found in the security advisories issued by Red Hat: <<https://rhn.redhat.com/errata/RHSA-2005-010.html>>

Recommended Actions:

For all system products which use vulnerable versions of VIM, Avaya recommends that customers restrict local access to the server. This restriction should be enforced through the use of physical security, firewalls, ACLs, VPNs, and other generally-accepted networking practices until such time as an update becomes available and can be installed. Furthermore, Avaya does not recommend local system users enable modeline or filetype plugins in VIM.

System Products with VIM installed:

Product	Affected S/W Version	Actions
Avaya™ S8700/S8710/S8500/S8300	All versions	Follow the recommended actions above.
Avaya™ Converged Communication Server	All versions	Follow the recommended actions above.
Avaya™ Network Routing (ANR)	All versions	Follow the recommended actions above.
Avaya™ MN100	All versions	Follow the recommended actions above.
Avaya™ Intuity LX	1.1-5.x	Follow the recommended actions above.
Avaya™ Message Storage Server (MSS)	All versions	Follow the recommended actions above.

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 CVLAN application does not require VIM. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.

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 25, 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.

© 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.