vim security update - (RHSA-2005-745)

Advisory Original Release Date: August 31, 2005
Last Revised: January 18, 2006
Number: ASA-2005-189
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

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. Although certain Avaya system products ship with vulnerable versions of VIM modelines are not enabled by default. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-2368 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-2005-745.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 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	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.
Avaya™ Integrated Management	All versions	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the Integrated Management application. 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.

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 31, 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.