

## xloadimage security update - (RHSA-2005-332)

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

**Last Revised:** January 18, 2006

**Number:** ASA-2005-134

**Risk Level:** Low

**Advisory Version:** 1.0

**Advisory Status:** Interim

### Overview:

The xloadimage utility displays images in an X Window System window, loads images into the root window, or writes images into a file. Xloadimage supports many image types (including GIF, TIFF, JPEG, XPM, and XBM).

Multiple security vulnerabilities were discovered in xloadimage. By persuading a local user to open malicious images using xloadimage, these vulnerabilities could allow an attacker to execute arbitrary code. Certain Avaya system products are affected by these vulnerabilities. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2005-0638](#) to this issue.

More information about these vulnerabilities can be found in the security advisory issued by Red Hat:

- <https://rhn.redhat.com/errata/RHSA-2005-332.html>

### Recommended Actions:

Until a patch is applied Avaya does not recommend customers open or view image files using xloadimage or xlie, from untrusted sources, on affected Avaya products.

### System Products with xloadimage installed:

Product	Affected S/W Version	Actions	Risk Level
Avaya™ Intuity LX	1.1-5.x	Follow the recommended actions above. An update is being considered for a future release.	Low
Avaya™ Modular Messaging MSS	All versions	Follow the recommended actions above. An update is being considered for a future release.	Low
Avaya™ MN100	All versions	Follow the recommended actions above. An update is being considered for a	Low

	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 vendors guidance:

**Software-Only Products**

Product	Affected S/W Version	Actions
Avaya™ CVLAN	All versions	<p>Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application.</p> <p>The CVLAN application does not require the software described in this advisory. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.</p>

**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 - June 14, 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](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.