Vulnerabilities in libtiff – (RHSA-2005-019)

Advisory Original Release Date: January 25, 2005
Last Revised: January 25, 2005
Number: ASA-2005-021
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

Overview:

Multiple security vulnerabilities were discovered in the libtiff package. If an attacker were to convince a local user on the system to open a carefully crafted image file, the vulnerabilities could execute arbitrary code in the application the image was opened with. Certain Avaya system products ship with libtiff and therefore are affected by this vulnerability. These vulnerabilities are separate from those covered in ASA-2005-002. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-1183 and CAN-2004-1308 to this issue.

More information about this vulnerability can be found in the security advisories issued by Red Hat <https://rhn.redhat.com/errata/RHSA-2005-019.html>.

Recommended Actions:

For all system products which use vulnerable versions of libtiff, 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. Additionally, Avaya recommends against the opening or viewing of TIFF images on the products listed below.

System Products with libtiff installed:

Product	**Affected S/W Version**	**Actions**
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 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 libtiff package may be installed on the Operating System upon which customers installed the CVLAN application. The CVLAN application does not require libtiff. 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 libtiff package may be installed on the Operating System upon which customers installed Integrated Management. Integrated Management does not require libtiff. 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 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.