

GTK2 and gdk-pixbuf Security Updates - (RHSA-2005-810 RHSA-2005-811)

Advisory Original Release Date: November 21, 2005

Last Revised: November 21, 2005

Number: ASA-2005-229

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Final

Overview:

The gtk2 package contains the GIMP ToolKit (GTK+), a library for creating graphical user interfaces for the X Window System.

The gdk-pixbuf package contains an image loading library utilized with the GNOME GUI desktop environment.

Several vulnerabilities were discovered in GTK2. Avaya system products do not ship with the GTK2 package and therefore are not affected by this vulnerability. There was an infinite-loop denial of service vulnerability reported in gdk-pixbuf package. If an attacker could trick a user into opening a carefully crafted XPM file, a linked application could be caused to stop responding. The Avaya Intuity LX, Avaya Message Networking, and Avaya Modular Messaging Message Storage Server ship with gdk-pixbuf. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names [CVE-2005-2975](#), [CVE-2005-2976](#), and [CVE-2005-3186](#) to these issues.

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

- <https://rhn.redhat.com/errata/RHSA-2005-810.html>
- <https://rhn.redhat.com/errata/RHSA-2005-811.html>

System Products which contain GTK2: None

System Products which contain gdk-pixbuf:

Product	Affected S/W Version	Actions	Risk Level
Avaya™ Intuity LX	All Versions	Follow recommended actions below. A patch is being considered for a future update.	Low
Avaya™ Message Networking	All Versions	Follow recommended actions below. A patch is being considered for a future update.	Low
Avaya™ Modular Messaging –	All Versions	Follow recommended actions below. A patch is being considered for a future update.	Low

MSS			
-----	--	--	--

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 vulnerabilities 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 effected packages 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 packages.</p>
Avaya Integrated Management (AIM)	All versions	<p>Depending on the Operating System provided by customers, the effected packages may be installed on the underlying Operating System supporting the AIM application.</p> <p>The AIM 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 packages.</p>

Recommended Actions:

For all system products which use vulnerable versions of gdk-pixbuf, 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.

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 1-800-242-2121, 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 - November 21, 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.