Xfree86 security update - (RHSA-2005-329 RHSA-2005-501)

Advisory Original Release Date: October 19, 2005
Last Revised: August 28, 2006
Number: ASA-2005-226
Risk Level: Low
Advisory Version: 2.0

Advisory Status: Interim

Overview:

XFree86 is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces (GUIs) such as GNOME and KDE are designed upon.

Several vulnerabilities have been discovered in the Xfree86. Several integer overflows have been found in the way that pixmap images are parsed by Xfree86 that could allow a remote attacker to elevate existing privileges. The Avaya Modular Messaging Message Storage Server, Avaya Message Networking, and the Avaya Intuity LX are vulnerable to this issue. The common vulnerabilities and exposures project (cve.mitre.org) has assigned the name CAN-2005-2495 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-2005-329.html
- https://rhn.redhat.com/errata/RHSA-2005-501.html

System Products utilizing Xfree86:

Product	Affected S/W Version	Actions	Risk Level
Avaya™ Modular Messaging Message Storage Server (MSS)	1.x – 2.x	Update to MSS 3.0 or later	Low
Avaya™ Message Networking	All	Follow recommended actions below. A patch is being considered for a future release.	Low
Avaya™ Intuity LX	All	Follow recommended actions below. A patch is being considered for a future release.	Low

Recommended Actions:

For all system products which use vulnerable versions of Xfree86, Avaya recommends that customers restrict local and network 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.

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 utilized 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).
Avaya™ Integrated Management	All versions	Depending on the Operating System provided by customers, the affected package may be utilized 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).

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 – October 19, 2005 – Initial statement issued.
V 2.0 - August 28, 2006 - Updated impact for MSS.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.