Updated fileutils/coreutils package fix ls vulnerabilties - (RHSA-2003-309)

Advisory Original Release Date: October 4, 2005
Last Revised: October 27, 2005
Number: ASA-2005-213
Risk Level: Medium
Advisory Version: 2.0

Advisory Status: Interim

Overview:

The fileutils package contains several basic system utilities. One of these utilities is the "ls" program, which is used to list information about files and directories.

Multiple vulnerabilities have been discovered in the fileutils *ls* command. Georgi Guninski discovered a memory starvation denial of service vulnerability in the *ls* program. A separate issue has been discovered in a non-exploitable integer overflow that could cause a system crash. A remote attacker could exploit either of these vulnerabilities to create a denial-of-service (DoS) on an affected system. The common vulnerabilities and exposures project (cve.mitre.org) has assigned the names CAN-2003-0853 and CAN-2003-0854 to these issues.

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

- https://rhn.redhat.com/errata/RHSA-2003-309.html

System Products utilizing fileutils:

Product	**Affected S/W Version**	**Actions**	**Risk Level**
Avaya™ S8710/S8700/S8500/S8300	Prior to CM 3.0.1 SP 10706	Fixes for this issue are included in CM 3.0.1 with SP 10706 and later. Avaya recommends that systems running Communication Manager release 3.0 and earlier take advantage of these security fixes by upgrading to CM 3.0.1 with SP 10706 and later. (see below for more information)	Medium
Avaya™ Converged Communication Server (CCS)	CCS - All versions	Follow recommended actions below. A patch is being considered for a future	Medium

		update.	

Recommended Actions for S8710/S8700/S8500/S8300 servers:

Avaya recommends that systems running Communication Manager release 3.0 and earlier take advantage of these security fixes by upgrading to CM 3.0.1 with SP 10706 and later. The Avaya Communication Manager Service pack instructions, release notes, and downloads are available from:

Avaya Communication Manager Service Packs for 3.0

Recommended Actions:

For all system products which use vulnerable versions of fileutils, 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 4, 2005 - Initial statement issued.
V 2.0 - October 27, 2005 - Corrected statement in Recommended actions from cpio to fileutils

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