

Vulnerability in ncompress - (RHSA-2004-536)

Advisory Original Release Date: January 18, 2005

Last Revised: July 21, 2005

Number: ASA-2005-015

Risk Level: Low

Advisory Version: 2.0

Advisory Status: Final

Overview:

A security vulnerability was discovered in ncompress. This vulnerability could allow an attacker the ability to execute arbitrary code by tricking a local system user into decompressing a carefully crafted filename. Certain Avaya system products ship with vulnerable versions of ncompress. However, ncompress is not used by any applications or network services. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2001-1413](#) to this issue.

More information about this vulnerability can be found in the security advisory issued by Red Hat <<https://rhn.redhat.com/errata/RHSA-2004-536.html>>.

July 2005 Update:

Avaya Communication Manager (CM) 2.2 Service Pack 10218 has been released which includes fixes to address the above issues in the Avaya S8710, S8700, S8500, and S8300 products. Please see the recommendations sections for more information.

System Products with ncompress installed:

Product	Affected S/W Version	Actions
Avaya™ S8710/S8700/S8500/S8300	All versions prior to CM2.2 SP10218	The affected package(s) were removed in the following releases and field loads: CM2.2 SP10218 CM3.0 Avaya recommends that systems running Communications Manager (CM) release 2.2 and earlier take advantage of these security fixes by upgrading to CM2.2 with SP 10218 (or later) or by upgrading to CM3.0 (see below for more information).
Avaya™ Converged Communication Server	All versions	Follow the recommended actions below. The affected package will be removed in future versions of the

		product.
Avaya™ Network Routing	All versions	Follow the recommended actions below. The affected package will be removed in future versions of the product.

Recommended Actions for S8710/S8700/S8500/S8300:

Avaya recommends that systems running Communications Manager release 2.2 and earlier take advantage of these security fixes by upgrading to CM2.2 with SP 10218 (or later) or by upgrading to CM3.0. The Avaya CM2.2 Service Packs instruction, release notes, and downloads are available from:

[Avaya Communication Manager Service Packs for 2.2](#)

Recommended Actions:

For all system products which use vulnerable versions of ncompress, 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. Furthermore, Avaya does not recommend the use of ncompress for compression or decompression of files (.Z extension).

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	The ncompress package may be installed on the Operating System upon which customers installed CVLAN. CVLAN does not require ncompress. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected application.
Avaya™	All versions	The ncompress package may be installed

Integrated Management	on the Operating System upon which customers installed Integrated Management. Integrated Management does not require ncompress. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or 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 1-800-242-2121, 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 - January 18, 2005 - Initial statement issued.
- V 2.0 - July 21, 2005 - CM 2.2 SP 10218 released.

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.