

rsh security update - (RHSA-2005-495 & RHSA-2005-074)

Advisory Original Release Date: August 29, 2005

Last Revised: August 29, 2005

Number: ASA-2005-167

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Final

Overview:

The rsh package contains a set of programs that allow users to run commands on remote machines, login to other machines, and copy files between machines, using the rsh, rlogin, and rcp commands. All three of these commands use rhosts-style authentication.

A security vulnerability was discovered in rsh (rcp). If a victim can be tricked into copying files from a malicious server using rcp, this vulnerability could allow an attacker to overwrite arbitrary files. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2005-0175](#) to these issues.

More information about this vulnerability can be found in the security advisories issued by Red Hat

- <https://rhn.redhat.com/errata/RHSA-2005-495.html>
- <https://rhn.redhat.com/errata/RHSA-2005-074.html>

Avaya System Products with rsh installed:

Product	Affected S/W Version	Comments and Actions
Avaya™ S8710/S8700/S8500/S8300	All versions	Prior to CM2.0, rcp (rsh) was utilized in server mode to receive files from the primary Avaya media server. CM2.0 and later do not utilize rcp and therefore Avaya recommends customer upgrade to CM2.0 or later.
Avaya™ Converged Communication Server	All versions	No Action Required. The affected package(s) will be removed in future versions of the product.

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. This vulnerability often does 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	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting CVLAN. CVLAN does not require the affected package. Avaya recommends that customers follow the recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.
Avaya Integrated Management (AIM)	All Versions	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the AIM application. Integrated Management does not require the affected package. Avaya recommends that customers follow the recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.

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 - August 29, 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.