

Vulnerability in glibc – (RHSA-2004-586)

Advisory Original Release Date: January 14, 2005

Last Revised: January 14, 2005

Number: ASA-2005-011

Risk Level: Low

Advisory Version: 1.1

Advisory Status: Interim

Overview:

A security vulnerability in the temporary file handling of the catchsegv script of glibc was discovered. This vulnerability could allow an attacker to overwrite files via a symlink attack. An attacker attempting to exploit this vulnerability would need local user access to the system. Furthermore, an attacker would need to convince a local privileged user to execute the catchsegv script in order to successfully exploit this vulnerability. Certain Avaya products utilize vulnerable versions of glibc; however, these systems do not utilize the catchsegv script. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2004-0968](#) 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-2004-586.html>>.

Recommended Actions:

For all system products which use vulnerable versions of glibc, 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.

System Products including glibc:

Product	Affected S/W Version	Actions
Avaya™ S8710/S8700/S8500/S8300	All versions	Follow the recommended actions above.
Avaya™ Converged Communication Server	All versions	Follow the recommended actions above.
Avaya™ Intuity LX	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.
Avaya™ Modular Messaging	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.

Avaya™ MN100	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.
Avaya™ Network Routing	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release.

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	No actions required. CLVAN is not affected by this vulnerably.

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 1-866-GO-AVAYA, 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 5, 2005 – Initial statement issued.

V 1.1 – April 5, 2005 – Incorrect CVE number fix.

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.