gzip security update - (RHSA-2005-357)

Advisory Original Release Date: August 29, 2005
Last Revised: August 22, 2006
Number: ASA-2005-172
Risk Level: Low
Advisory Version: 2.0

Advisory Status: Interim

Overview:

The gzip package contains the GNU gzip data compression program.

Multiple security vulnerabilities were discovered in gzip. If a local user is tricked into executing zgrep or gunzip on a malicious file, these vulnerabilities could allow an attacker to execute arbitrary commands or overwrite arbitrary files. Certain Avaya product ship with and utilize gzip, for delivering software updates, and therefore are affected by these vulnerabilities. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2005-0758, CAN-2005-0988, and CAN-2005-1228 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-2005-357.html

Avaya System Products with gzip installed:

Product	Affected S/W Version	Comments and Actions
Avaya™ S8710/S8700/S8500/S8300	All versions	An update is being considered for a future version.
Avaya™ Converged Communication Server	All versions	An update is being considered for a future version.
Avaya™ Intuity LX	Versions 1.1-5.x	An update is being considered for a future version.
Avaya™ Modular Messaging – Message Storage Server (MSS)	Version 1.x-2.x	Upgrade to MSS 3.0 or later.
Avaya™ Network Messaging	All versions	An update is being considered for a future version.

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 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	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting CVLAN. Avaya recommends that customers follow the recommended actions supplied by the Operating System vendor (e.g. Red Hat).
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. Avaya recommends that customers follow the 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.

Revision History:

V 1.0 - August 29, 2005 - Initial statement issued.
V 2.0 - August 22, 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.