

## Updated zip packages fix security issues – (RHSA-2004-634)

**Advisory Original Release Date:** January 25, 2005

**Last Revised:** January 25, 2005

**Number:** ASA-2005-019

**Risk Level:** Low

**Advisory Version:** 1.0

**Advisory Status:** Interim

### Overview:

A security vulnerability was discovered in zip. This vulnerability could allow an attacker the ability to execute arbitrary code by tricking a local system user into unzipping a carefully crafted file. Certain Avaya system products ship with vulnerable versions of zip. However, zip is not used by any applications or network services. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2004-1010](#) to this issue.

More information about these vulnerabilities can be found in the security advisories issued by Red Hat: <<https://rhn.redhat.com/errata/RHSA-2004-634.html>>

### Recommended Actions:

For all system products which use vulnerable versions of zip, 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 zip for compression or decompression of files (.zip extension).

### System Products with Zip installed:

Product	Affected S/W Version	Actions
Avaya™ Network Routing	All versions	Follow the recommended actions above. The affected package will be removed in future versions of the product.
Avaya™ MN100	All versions	Follow the recommended actions above. The affected package will be removed in future versions of the product.
Avaya™ Intuity LX	1.1-5.x	Follow the recommended actions above. The affected package will be removed in future versions of the product.
Avaya™ Modular Messaging MSS	All versions	Follow the recommended actions above. The affected package 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. 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**

<b>Product</b>	<b>Affected S/W Version</b>	<b>Actions</b>
Avaya™ CVLAN	All versions	The CVLAN application does not require Zip. Avaya recommends that customers follow 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 1-866-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 25, 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](mailto: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.