

tcpdump security update - (RHSA-2005-417 & RHSA-2005-421)

Advisory Original Release Date: June 14, 2005

Last Revised: August 31, 2006

Number: ASA-2005-137

Risk Level: Low

Advisory Version: 3.0

Advisory Status: Interim

Overview:

Tcpdump is a command-line tool for monitoring network traffic.

Multiple security vulnerabilities were discovered in tcpdump. These vulnerabilities could allow an attacker to crash listening tcpdump by injecting malicious onto the network. Certain Avaya products ship with tcpdump installed, for debugging purposes, and therefore are affected by some of these vulnerabilities. In order for an attacker to exploit these vulnerabilities, an authenticated local system user would first have to manually start the tcpdump application. On Avaya system products, tcpdump access is restricted to Avaya Service technicians.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CAN-2005-1278](#), [CAN-2005-1279](#), and [CAN-2005-1280](#) to these issues.

More information about these vulnerabilities can be found in the security advisory issued by Red Hat:

- <https://rhn.redhat.com/errata/RHSA-2005-417.html>
- <https://rhn.redhat.com/errata/RHSA-2005-421.html>

System Products with tcpdump installed:

Product	Affected S/W Version	Actions	Risk Level
Avaya™ S8710/S8700/S8500/S8300	Versions prior to CM 3.1	Avaya recommends upgrading to CM 3.1 to address this issue.	Low
Avaya™ Converged Communications Systems (CCS)	All Versions	An update is being considered for a future release.	Low
Avaya™ Intuity LX	1.1-5.x	An update is being considered for a future release.	Low
Avaya™ Modular Messaging MSS	1.0-2.x	Upgrade to MSS 3.0 or later.	Low
Avaya™ MN100	All versions	An update is being considered for a future release.	Low

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	<p>Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application.</p> <p>The CVLAN application does not require the software described in this advisory. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.</p>

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 – June 14, 2005 – Initial statement issued.
- V 2.0 – August 22, 2006 – Updated impact for MSS.
- V 3.0 – August 31, 2006 – Updated actions for S8xx0

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.

© 2006 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.