

---

## Wireshark security and bug fix update (RHSA-2007-0709)

Original Release Date: January 2, 2008

Last Revised: September 9, 2008

Number: ASA-2007-525

Risk Level: Low

Advisory Version: 2.0

Advisory Status: Final

---

### 1. Overview:

Wireshark is a network packet sniffing and packet analyzing utility.

Wireshark was found to contain numerous Denial of Service (DoS) issues in the protocol dissectors for the HTTP, iSeries, DCP ETSI, SSL, MMS, DHCP and BOOTP protocols when reading packets live from the network. The Common Vulnerabilities and Exposures project ([cve.mitre.org](http://cve.mitre.org)) has assigned the names [CVE-2007-3389](#), [CVE-2007-3390](#), [CVE-2007-3391](#) and [CVE-2007-3392](#), to these issues.

More information about these vulnerabilities can be found in the security advisory issued by RedHat Linux:

- <https://rhn.redhat.com/errata/RHSA-2007-0709.html>

### 2. Avaya System Products with Wireshark installed:

Product:	Affected Version(s):	Risk Level:	Actions:
Avaya Communication Manager	CM 3.x, 4.x, 5.0	Low	Upgrade to CM 5.1 or later.
Avaya CCS/SES	SES 3.1.x, 4.0, 5.0	Low	Upgrade to SES 5.1 or later.

### 3. 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.

<b>Product:</b>	<b>Actions:</b>
CVLAN	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application. The CVLAN application does not require the software described in this advisory.
Avaya Integrated Management Suite (IMS)	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the IMS application. The IMS application does not require the software described in this advisory.

#### **Recommended Actions:**

In the event that the affected package is installed, Avaya recommends that customers follow recommended actions supplied by RedHat Linux.

## **4. Additional Information:**

Additional information may also be available via the Avaya support [website](#) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

## **5. 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 BUT NOT LIMITED TO 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, INCIDENTAL, STATUTORY, 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.

## **6. Revision History:**

V 1.0 - January 2, 2008 - Initial Statement issued.

V 2.0 - September 9, 2008 - Changed CM and SES affected versions and recommended actions, changed ASA status.

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).

© 2007 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.