Ethereal security update - (RHSA-2005-809)

Advisory Original Release Date: October 28, 2005
Last Revised: October 28, 2005
Number: ASA-2005-227
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

Overview:

Ethereal (tethereal) is a program for monitoring network traffic.

Multiple security vulnerabilities were discovered in Ethereal. On a system where Ethereal is running, a remote attacker could send malicious packets that could cause Ethereal to crash or execute arbitrary code. Certain Avaya products ship with Ethereal (tethereal) 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 Ethereal (tethereal) application. On Avaya system products, Ethereal (tethereal) access is restricted to Avaya Service technicians. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the CVE-2005-3184, CVE-2005-3241, CVE-2005-3242, CVE-2005-3243, CVE-2005-3244, CVE-2005-3245, CVE-2005-3246, CVE-2005-3247, CVE-2005-3248, and CVE-2005-3249 to these issues

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

- https://rhn.redhat.com/errata/RHSA-2005-809.html

Recommended Actions: None

System Products with Ethereal installed:

Product	**Affected S/W Version**	**Actions**
Avaya™ S8710/S8700/S8500/S8300	All versions	An update is being considered for a future release. Avaya media servers are affected by the following by the following vulnerabilities: CVE-2005-3184, CVE-2005-3241, CVE-2005-3242, CVE-2005-3243, CVE-2005-3244, CVE-2005-3245, CVE-2005-3246, CVE-2005-3247, CVE-2005-3248, and CVE-2005-3249

Avaya™ Converged Communication Server (CCS)/ SIP Enablement Services (SES)	All versions	An update is being considered for a future release. Avaya media servers are affected by the following by the following vulnerabilities: CVE-2005-3184, CVE-2005-3241, CVE-2005-3242, CVE-2005-3243, CVE-2005-3244, CVE-2005-3245, CVE-2005-3246, CVE-2005-3247, CVE-2005-3248, and CVE-2005-3249

Further information regarding the Ethereal vulnerabilities on Avaya system products is below:

CVE-2005-3184 - A buffer overflow vulnerability in the unicode_to_bytes in the Service Location Protocol (srvloc) dissector (packet-srvloc.c) allows remote attackers to execute arbitrary code via a srvloc packet with a modified length value. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3241 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3242 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3243 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3244 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3245 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3246 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3247 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3248 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CVE-2005-3249 - This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

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.

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 - October 28, 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.