Ethereal security update - (RHSA-2005-687)

Advisory Original Release Date: August 30, 2005
Last Revised: August 30, 2005
Number: ASA-2005-185
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 names CAN-2005-2360, CAN-2005-2361, CAN-2005-2362, CAN-2005-2363, CAN-2005-2364, CAN-2005-2365, CAN-2005-2366, and CAN-2005-2367 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-2005-687.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: CAN-2005-2360, CAN-2005-2361, CAN-2005-2362, CAN-2005-2363, CAN-2005-2364, CAN-2005-2365, and CAN-2005-2367
Avaya™ Converged	All versions	An update is being considered for a

Communication Server		future release. Avaya media servers are affected by the following by the following vulnerabilities: CAN-2005-2360, CAN-2005-2361, CAN-2005-2362, CAN-2005-2363, CAN-2005-2364, CAN-2005-2365, and CAN-2005-2367

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

CAN-2005-2360 - A vulnerability in the LDAP dissector in Ethereal 0.8.5 through 0.10.11 could allow remote attackers to cause a denial of service (free static memory and application crash) via unknown attack vectors. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-2361 - A vulnerability in the AgentX dissector, PER dissector, DOCSIS dissector, SCTP graphs, HTTP dissector, DCERPC, DHCP, RADIUS dissector, Telnet dissector, IS-IS LSP dissector, or NCP dissector in Ethereal 0.8.19 through 0.10.11 could allow remote attackers to cause a denial of service (application crash or abort). This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-2362 - A vulnerability in several dissectors in Ethereal 0.9.0 through 0.10.11 allows remote attackers to cause a denial of service (application crash) by reassembling certain packets. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-2363 - A vulnerability in the SMPP dissector, 802.3 dissector, DHCP, MEGACO dissector, or H1 dissector in Ethereal 0.8.15 through 0.10.11 allows remote attackers to cause a denial of service (infinite loop). This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-2364 - A vulnerability in the GIOP dissector, WBXML, or CAMEL dissector in Ethereal 0.8.20 through 0.10.11 allows remote attackers to cause a denial of service (application crash) via certain packets that cause a null pointer dereference. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-2365 - A vulnerability in the SMB dissector in Ethereal 0.9.0 through 0.10.11 allows remote attackers to cause a buffer overflow or a denial of service (memory consumption) via unknown attack vectors. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-2366 - A vulnerability in the BER dissector in Ethereal 0.10.11 allows remote attackers to cause a denial of service (abort or infinite loop). Avaya

media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-2367 - A format string vulnerability in the proto_item_set_text function in Ethereal 0.9.4 through 0.10.11, as used in multiple dissectors, allows remote attackers to write to arbitrary memory locations and gain privileges via a crafted AFP packet. 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 - August 30, 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.