Ethereal security update - (RHSA-2005-306 & RHSA-2005-427)

Advisory Original Release Date: June 13, 2005
Last Revised: January 18, 2006
Number: ASA-2005-131
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.

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

- https://rhn.redhat.com/errata/RHSA-2005-306.html
- https://rhn.redhat.com/errata/RHSA-2005-427.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-2005-0699, CAN-2005-0739, CAN-2005-1456, CAN-2005-1457, CAN-2005-1459, CAN-2005-1461, CAN-2005-1464, CAN-2005-1467, CAN-2005-1468, and CAN-2005-1470
Avaya™ Converged Communication Server	All versions	An update is being considered for a future release.

		Avaya media servers are affected by the following by the following vulnerabilities: CAN-2005-0699, CAN-2005-0739, CAN-2005-1456, CAN-2005-1457, CAN-2005-1459, CAN-2005-1461, CAN-2005-1464, CAN-2005-1467, CAN-2005-1468, and CAN-2005-1470

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

CAN-2005-0699 - Multiple buffer overflows in the dissect_a11_radius function in the CDMA A11 (3G-A11) dissector (packet-3g-a11.c) for Ethereal 0.10.9 and earlier could allow remote attackers to execute arbitrary code via RADIUS authentication packets with large length values. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-0704 - Buffer overflow in the Etheric dissector in Ethereal 0.10.7 through 0.10.9 could allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-0705 - The GPRS-LLC dissector in Ethereal 0.10.7 through 0.10.9, with the "ignore cipher bit" option enabled, could allow remote attackers to cause a denial of service (application crash). Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-0739 - Mutliple buffer overflows in the IAPP dissector (packet-iapp.c) for Ethereal 0.9.1 to 0.10.9 could allow remote attackers to execute arbitrary code via malicious length values. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-0765 - A vulnerability in the JXTA dissector for Ethereal 0.10.9 could allow a remote attackers to cause a denial of service (application crash). Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-0766 - A vulnerability in the sFlow dissector in Ethereal 0.9.14 through 0.10.9 could allow remote attackers to cause a denial of service (application crash). Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1456 - Multiple vulnerabilities in the DHCP and Telnet dissectors in Ethereal 0.9.10 through 0.10.10 could allow remote attackers to cause a denial of service (abort). The DHCP vulnerability does not affect Avaya media servers since they do no ship with the affected versions of Ethereal (tethereal). The Telnet dissector vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1457 - Multiple vulnerabilities in the AIM, LDAP, FibreChannel, GSM_MAP, SRVLOC, and NTLMSSP dissectors in Ethereal 0.9.7 through 0.10.10 could allow remote attackers to cause a denial of service (application crash). The AIM, LDAP, and GSM_MAP vulnerabilities do not affect Avaya media servers since the affected version of Ethereal (tethereal) do ship with Avaya products. The FibreChannel, SRVLOC, and NTMLSSP vulnerabilities affect the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1458 - Multiple vulnerabilities in the KINK dissector in Ethereal (0.10.10) could allow remote attackers to cause a denial of service and possible execute arbitrary code. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1459 - Multiple unknown vulnerabilities in the WSP, BER, SMB, NDPS, IAX2, RADIUS, TCAP, MRDISC, 802.3 Slow, SMBMailslot, and SMB PIPE dissectors in Ethereal 0.8.19 through 0.10.10 could allow remote attackers to cause a denial of service (assert error). The WSP, BER, IAX2, RADIUS, TCAP, and 802.3 Slow vulnerabilities do not affect Avaya media servers since the affected version of Ethereal (tethereal) do ship with Avaya products. The SMB, NDPS, MRDISC, SMBMailslot, and SMB PIPE vulnerabilities affect the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1460 - Multiple dissectors in Ethereal 0.10.8 through 0.10.10 could allow remote attackers to cause a denial of service (assert error) via an invalid protocol tree item length. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1461 - Multiple buffer overflows in the SIP, CMIP, CMP, CMS, CRMF, ESS, OCSP, X.509, ISIS, DISTCC, FCELS, Q.931, NCP, TCAP, ISUP, MEGACO, PKIX1Explitit, PKIX_Qualified, and Presentation dissectors in Ethereal before 0.10.11 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code. The SIP, CMIP, CMP, CMS, CRMF, ESS, OCSP, PKIX1Explitit, PKIX Qualified, X.509, Q.931, NCP, TCAP, and MEGACO vulnerabilities do not affect Avaya media servers since the affected version of Ethereal (tethereal) do ship with Avaya products. The ISIS, DISTCC, FCELS, ISUP, vulnerabilities affect the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1462 - A double-free vulnerability in the ICEP dissector in Ethereal 0.10.7 to 0.10.10 could allow remote attackers to execute arbitrary code. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1463 - Multiple format string vulnerabilities in the (1) DHCP and (2) ANSI A dissectors in Ethereal 0.9.15 through 0.10.10 could allow remote attackers to execute arbitrary code. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1464 - Multiple vulnerabilities in the KINK, L2TP, MGCP, EIGRP, DLSw, MEGACO, LMP, and RSVP dissectors in Ethereal 0.8.14 through 0.10.10 could allow remote attackers to cause a denial of service (infinite loop). The KINK, L2TP, and MEGACO vulnerabilities do not affect Avaya media servers since the affected version of Ethereal (tethereal) do ship with Avaya products. The MGCP, EIGRP, DLSw, LSP, and RSVP vulnerabilities affect the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1465 - A vulnerability in the NCP dissector in Ethereal 0.10.5 through 0.10.10 could allow remote attackers to cause a denial of service. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1466 - A vulnerability in the DICOM dissector in Ethereal 0.10.4 through 0.10.10 could allow remote attackers to cause a denial of service. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1467 - A vulnerability in the NDPS dissector in Ethereal 0.9.12 through 0.10.10 could allow remote attackers to cause a denial of service. This vulnerability affects the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1468 - Multiple vulnerabilities in the WSP, Q.931, H.245, KINK, MGCP, RPC, SMBMailslot, and SMB NETLOGON Ethereal could allow remote attackers to cause a denial of service. The WSP, KINK, Q.931, and H.245 vulnerabilities do not affect Avaya media servers since the affected version of Ethereal (tethereal) do ship with Avaya products. The MGCP, SMBMailslot, SMB NETLOGON, and RPC vulnerabilities affect the Avaya Converged Communication Server and the S8710/S8700/S8500/S8300 media servers.

CAN-2005-1469 - A vulnerability in the GSM dissector in Ethereal 0.10.10 could allow remote attackers to cause the dissector to access an invalid pointer. Avaya media servers do no ship with the affected versions of Ethereal (tethereal) and are therefore not affected by this vulnerability.

CAN-2005-1470 - Multiple vulnerabilities in the TZSP, MGCP, ISUP, SMB, and Bittorrent dissectors in Ethereal before 0.10.11 allow remote attackers to cause a denial of service (segmentation fault) via unknown vectors. The TZSP and Bittorrent vulnerabilities do not affect Avaya media servers since the affected version of Ethereal (tethereal) do ship with Avaya products. The MGCP, ISUP, SMB, and vulnerabilities affect 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 1-866-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

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 13, 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.