TCP does not adequately validate segments before updating timestamp value (CERT-637934)

Advisory Original Release Date: June 29, 2005
Last Revised: June 29, 2005
Number: ASA-2005-148
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

Overview: A vulnerability has been identified in the TCP protocol with timestamps when using the PAWS algorithm. An attacker could exploit this vulnerability by carefully crafting packets and injecting them into the data stream causing a denial of service. Some Avaya system products are affected by this vulnerability.

More information about this vulnerability can be found in the following links:

- http://www.kb.cert.org/vuls/id/637934
- http://seclists.org/lists/fulldisclosure/2005/May/0526.html

System Products which utilize TCP Timestamps with PAWS:

Product	Affected S/W Version	Risk	Comments
Avaya™ G250/G350/ G700	All Versions	Low	Avaya will provide patches in the next major release as available.
Modular Messaging (MSS Only)	All Versions	Low	Avaya will provide patches in the next major release as available.
Avaya NM100	1.x-2	Low	Avaya will provide patches in the next major release as available.
Avaya Intuity LX	1.1-5.x	Low	Avaya will provide patches in the next major release as available.
Avaya IP Phones	1.x-2.1	Low	TCP timestamps are turned off beginning in firmware R2.2. Avaya recommends upgrading IP phones to R2.2 as applicable.

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	Depending on the Operating System provided by customers, the effected package may be installed on the underlying Operating System supporting the CVLAN application. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat).
Avaya Integrated Management/ System Management (IM/SM)	All Versions	Depending on the Operating System provided by customers, the effected package may be installed on the underlying Operating System supporting the IM/SM application. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat).

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 29, 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.