Talkpath issue for TN2602AP IP Media Resource 320

Advisory Original Release Date: November 30, 2005
Last Revised: April 11, 2006
Number: ASA-2005-231
Risk Level: Medium
Advisory Version: 2.0

Advisory Status: Final

Overview:

The TN2602AP IP Media Resource 320 circuit pack provides high-capacity Voice over Internet (VoIP) protocol audio access to the switch for local stations and outside trunks.

A flaw was discovered in the Avaya TN2602AP IP Media Resource 320 prior to vintage 9 firmware. This flaw could allow a remote attacker to cause a denial of service (memory leak) via specially crafted packets. Although Avaya is not aware of active attacks that exploit this flaw, customers are recommended to upgrade to vintage 9 firmware (or later) to resolve this issue. The common vulnerabilities and exposures project (cve.mitre.org) has assigned the name CVE-2005-3989 to this issue.

System Products:

Product	Affected S/W Version	Actions	Risk Level
Avaya™ TN2602AP IP Media Resources 320 circuit pack	All Versions prior to vintage 9 firmware	Upgrade to vintage 9 firmware (or later) by following the instructions below.	Medium

Recommended Actions for TN2602AP IP Media Resources 320:

Upgrade to vintage 9 firmware (or later) by following the instructions located at:

http://support.avaya.com/japple/css/japple?temp.documentID=236667&temp.productID=136527&temp.releaseID=228560&temp.bucketID=108025&PAGE=Document#TN2602

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 - November 30, 2005 - Initial statement issued.
V 2.0 - April 11, 2006 - Added CVE number to the advisory.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.

© 2005 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.