SCO UnixWare telnet client multiple issues - (SCOSA-2005.21)

Advisory Original Release Date: July 14, 2005
Last Revised: August 2, 2005
Number: ASA-2005-156
Risk Level: Low
Advisory Version: 2.0

Advisory Status: Interim

Overview:

SCO has announced multiple vulnerabilities in the Telnet client

Multiple security vulnerabilities were discovered in telnet. If a victim can be tricked into connecting to a malicious telnet server, these vulnerabilities could allow an attacker to execute arbitrary code on a victim's machine. Certain Avaya products ship with the telnet package and therefore are affected by these vulnerabilities. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0468 and CAN-2005-0469 to these issues.

More information about this vulnerabilities can be found in the security advisory issued by SCO for Unixware based systems.

- ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.21/SCOSA-2005.21.txt

Avaya SCO Unixware based System Products which use the telnet client:

Product	Affected S/W Version	Risk Level	Actions
Avaya™ Intuity Audix (Not including Intuity LX)	4.x-5.x	Low	Avaya recommends disabling telnet and utilizing ssh to mitigate this risk. An update is being considered for a future release.

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 - July 14, 2005 - Original Issue.
V 2.0 - August 2, 2005 - Changed state from Final to Interim

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