cpio race condition - (SCOSA-2005.32)

Advisory Original Release Date: September 6, 2005
Last Revised: September 6, 2005
Number: ASA-2005-191
Risk Level: Medium
Advisory Version: 1.0

Advisory Status: Interim

Overview:

SCO has announced two vulnerabilities in Unixware with cpio that could allow for:

1) A malicious local user to modify permissions of arbitrary files while being decompressed.

2) A malicious attacker to traverse the directory structure and write to arbitrary directories using a .. (dot)(dot) in a cpio file.

cpio is an application that copies files into or out of cpio or tar archives.

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

- ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32/SCOSA-2005.32.txt

The Common Vulnerabilities and Exposures Project (cve.mitre.org) has named these issues CAN-2005-1111 and CAN-2005-1229.

Avaya SCO Unixware based System Products which utilize cpio:

SCO Advisory	Affected S/W Version	Risk	Recommended Actions
SCOSA-2005.32	Intuity Audix R5	Medium	See Recommended Actions below. External firewall protection should be considered to mitigate risk of this vulnerability.

Recommended Actions: As described in the table above**, Intuity R5** is affected by the advisory described by SCO. This issue is intended to be addressed in the next major release of Intuity Audix. In the meantime, customers are encouraged to use generally-accepted secure networking practices (such as using ACLs, firewalls, etc.) to limit access to their Intuity Audix servers which are using the aforementioned network services so to minimize the risk of exploitation. If more information becomes available, this advisory will be updated.

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 - September 6, 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.