SCO UnixWare TCP connection reset vulnerability - (SCOSA-2005.14)

Advisory Original Release Date: May 5, 2005
Last Revised: May 5, 2005
Number: ASA-2005-097
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

Overview:

SCO has announced Unixware patches to address security issues with long-lived TCP connections. This vulnerability can allow remote attackers to disconnect/disrupt TCP based services like BGP that rely on long-lived sessions.

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-2005.14/SCOSA-2005.14.txt

TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

Reference : NISCC Vulnerability Advisory 236929
Reference : CERT Technical Cyber Security Alert TA04-111A

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0230 to this issue.

Avaya System Products using SCO Unixware TCP stack: Avaya system products include an Operating System with the product when it is delivered. The **Avaya Intuity Audix voicemail** system is delivered with a SCO Unixware Operating System.

Affected S/W Version	Risk	Recommended Actions
Intuity Audix R5	Low	Intuity Audix systems already ship with a very small value (4096) for default TCP Window Size, and do not utilize long-lived TCP based applications like BGP. This combination greatly reduces likelihood of TCP connection resets and makes this a low risk vulnerability for Intuity Audix systems. The SCO patch provides additional parameter tuning for rate limiting fragmented/out of sequence TCP packets for mitigating this

		attack. Avaya is investigating the impacts of this patch and intends to address this in the next major release of Intuity Audix. To further reduce the potential of connection resets, customers are encouraged to use generally-accepted secure networking practices (such as using ACLs, firewalls, etc.) to limit access to their Intuity Audix servers. 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 1-866-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 - May 5, 2005 – Initial statement issues.

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