ICMP Attacks against TCP (NISCC-532967)

Advisory Original Release Date: April 25, 2005
Last Revised: April 27, 2005
Number: ASA-2005-076
Risk Level: Medium
Advisory Version: 2.0

Advisory Status: Interim

Overview:

Multiple TCP/IP and ICMP implementations allow remote attackers to cause a denial of service via spoofed ICMP messages. These vulnerabilities are separated into three related but unique issues: (1) Blind TCP connection reset attacks utilizing spoofed ICMP Destination Unreachable messages, (2) Blind throughput-reduction attacks utilizing spoofing ICMP Source Quench messages, and (3) Blind throughput-reduction attacks utilizing spoofed ICMP Path MTU (PMTU) messages. Certain Avaya products are affected by these vulnerabilities. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0790, CAN-2004-0791, CAN-2004-1060, CAN-2005-0065, CAN-2005-0066, CAN-2005-0067, and CAN-2004-0068 to these issues.

More information about this vulnerability can be found in the following links: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en

As more information becomes available, this advisory will be updated.

System Products responses:

Product	Affected S/W Version	Comments and Actions
Avaya™ S8710/S8700/S8500/ S8300	None	TCP sequence numbers are verified in ICMP errors and connections will never abort due to a received ICMP packet. Therefore, Avaya media servers are not affected by any of these vulnerabilities.
Avaya™ Converged Communications Server	None	TCP sequence numbers are verified in ICMP errors and connections will never abort due to a received ICMP packet. Therefore, Avaya media servers are not affected by any of these vulnerabilities.
Avaya™ Intuity LX	None	TCP sequence numbers are verified in ICMP errors and connections will never abort due to a received ICMP packet. Therefore, Avaya media servers are not affected by these vulnerabilities.
Avaya™ MN100	None	TCP sequence numbers are verified in ICMP errors and connections will never abort due to a received ICMP packet. Therefore,

		Avaya media servers are not affected by these vulnerabilities.
Avaya™ Message Storage Server (MSS)	None	TCP sequence numbers are verified in ICMP errors and connections will never abort due to a received ICMP packet. Therefore, Avaya media servers are not affected by these vulnerabilities.
Avaya™ 46xx IP Phones	All Versions	Avaya™ IP Phones are only affected by blind throughput-reduction attacks utilizing spoofed ICMP Source Quench and PMTU messages (issues 2 and 3, respectively). Although exploitation of these vulnerabilities does not reset TCP connections it may impact the performance of network-based communications. Avaya is awaiting a patch from Wind Rivers. Once this patch is available, integrated, and certified this advisory will be updated to note the release of updated firmware versions.
Avaya™ SG 5, SG 5x, SG 200, SG 203 and SG 208	Versions 4.5.54 and earlier	Avaya™ SG products are only affected by blind throughput-reduction attacks utilizing spoofed ICMP Source Quench and PMTU messages (issues 2 and 3, respectively). Although exploitation of these vulnerabilities does not reset TCP connections it may impact the performance of network-based communications. Avaya plans to release a VPNos 4.x update to resolve these vulnerabilities. In the interim Avaya recommends customers configure blocking of ICMP Source Quench and PMTU messages as described below in the Recommended Actions section below.
Avaya™ VSU-100, VSU-2000, VSU-5000, VSU-7500 and VSU-10000.	Versions 3.2.38 and earlier	Avaya™ VSU products are only affected by blind throughput-reduction attacks utilizing spoofed ICMP Source Quench (issue 2). Although exploitation of this vulnerability does not reset TCP connections it may impact the performance of network-based communications. Avaya plans to release VPNos version 3.2.x to resolve this vulnerability. In the interim Avaya recommends customers configure blocking of ICMP Source Quench messages as described below in the Recommended Actions section below.
Unified Communications	All Versions	Follow Microsoft's recommendation for installing the Operating System patches

Center (UCC) - S3400		supplied in MS05-019. For more information see Avaya Security Advisory ASA-2005-073.
Modular Messaging - Messaging Application Server (MAS)	All Versions	Follow Microsoft's recommendation for installing the Operating System patches supplied in MS05-019. For more information see Avaya Security Advisory ASA-2005-073.
S8100/DefinityOne/IP 600 Media Servers	All Versions	Follow Microsoft's recommendation for installing the Operating System patches supplied in MS05-019. For more information see Avaya Security Advisory ASA-2005-073.
Call Management System (CMS)	All Versions	A patch from SUN is pending, no current workaround is available. For more information see SUN alert 57746
Interactive Response (IR)	All Version	A patch from SUN is pending, no current workaround is available. For more information see SUN alert 57746

Mitigating Factors:

General:

In order to exploit these vulnerabilities, an attacker must first predict or learn the IP address and port information of the source and the destination of an existing TCP network connection. In addition, an attack would have to be performed on each TCP connection that was targeted for reset. Many connections will automatically be restored if a reset attack is successful.

Avaya™ SG and VSU Products:

The attacks outlined above have no affect on Avaya™ SGs or VSUs ability to negotiate or sustain IPSec tunnels. In general, these attacks can only be mounted against VPNmanager, Client-Configuration-Download (CCD), and Secure Shell connections to VSUs and SGs. Since the majority of TCP connections to the SGs and VSUs are not long term the risk of an attack is reduced.

Recommended Actions:

Avaya™ SGs and VSUs:

Avaya recommends that customers block ICMP Source Quench and PMTU message using the product's firewall. The link below outlines the steps necessary to block ICMP messages in SG and VSU devices:

Configuring SG and VSU devices against ICMP Vulnerabilities [PDF]

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:

Avaya Software-Only Product installed on Microsoft Windows:

Follow Microsoft's recommendation for installing the Operating System patches supplied in MS05-019. For more information see Avaya Security Advisory ASA-2005-073.

Software-Only Products:

Product	Affected S/W Version	Actions
Avaya™ CVLAN	All versions	Both the Linux 2.4 and 2.6 kernels verify TCP sequence numbers in ICMP errors and connections will never abort due to a received ICMP packet. Therefore, Avaya™ CVLAN is not affected by these vulnerabilities. In addition, the CVLAN application does not require ICMP Source Quench or ICMP PMTU Discovery messages. Therefore, these messages can be blocked via network Access Control Lists (ACLs) or disabled in the underlying Operating System CVLAN is executing on. 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.

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 - April 25, 2005 - Initial statement issued.
V 2.0 - April 27, 2005 - Appended information for CMS and IR

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