Vulnerability Issues in Implementations of the H.323 Protocol

Advisory Original Release Date: January 13, 2004
Last Revised: July 26, 2004
Number: 04-02
Advisory Version: 2.0

Advisory Status: Interim

Overview:

Recently the U.K. National Infrastructure Security Co-ordination Centre (NISCC) issued an advisory concerning vulnerabilities that have been found in implementations of the H.323 protocol. A test suite created by the University of Oulu Security Programming Group (OUSPG) was used to discover the vulnerabilities. OUSPG has created test suites in the past to test other protocols and has recently produced a test suite for H.225, which is a part of the H.323 protocol family.

Avaya includes the H.323 protocol in certain products to support the delivery of IP telephony capabilities. The test suite created by OUSPG is being used by Avaya as another method of assessing possible vulnerabilities in the implementation of the H.323 protocol. An investigation of impact of the test cases on Avaya products is being conducted. Findings are reflected in the details below.

Details:

The following products utilize the H.323 protocol and have been found to be vulnerable to test cases implemented by the OUSPG tool. A successful exploit may be used to create a denial of service attack against a vulnerable device.

Avaya Products	Version	Status	Actions
SG5/ 5x/ 200/ 203/ 208	4.2, 4.3, 4.31.29	Vulnerable when the H.323 aware NAT capability is enabled	An upgrade to VPNos 4.4 will be required to resolve the vulnerability. **Mitigating Actions:** The H.323 capability is turned off by default. If the H.323 aware NAT capability is being used, reconfiguring the H.323 aware NAT to use ports other than the default ports of 1719 and 1720 can reduce the threat of an exploit.
Communication Manager Servers S8700, S8500,	All versions	Please perform the recommended actions until a software	Under certain circumstances, and when coupled with additional attack types, the Communication Manager server will reboot when subjected to test cases provided in the H.323

S8300, S8100, DEFINITY Server R, and DEFINITY Server SI/CSI		update is available. Software update status can be found in the update section below.	test-suit from OUSPG. Exploitation of these vulnerabilities may result in the execution of arbitrary code or cause a denial of service, which in some cases may require a system reboot. Similar vulnerabilities have been found to exist with the S8700, S8500, S8300, S8100, DEFINITY Server R, and DEFINITY Server SI/CSI. Avaya is currently working on fixes for these vulnerabilities. This advisory will be updated, as more information is available. Refer to the update section below for detailed software update status. **Mitigating Factors:** Successful H.323 attacks can only be launched from IP addresses known to Communication Manager. In order for a device to be recognized as a known entity, its IP address must be configured as a H.323 client, H.323 gateway, or trunk. This includes registered endpoints and administered signaling groups. If Communication Manager receives H.323 messages from an unknown entity, the TCP session will be closed before the H.225.0 message is processed. **Recommended Actions:** The following actions are recommended to help mitigate effects of an attempted H.323 attack: • Far-end-unspecified signaling groups are highly discouraged in non-Internet Call Centres. These signaling groups allow unknown entities to connect and communicate with Communication Manager. Removing far-end-unspecified signaling groups will restrict successful attacks to devices known to

			Communication Manager. • Apply network packet filters to block access to interfaces that should not accept H.323 services. Blocking ports 1720/TCP and 1720/UDP at a perimeter router/gateway will help to protect from an Internet-based attack. • Apply Access Control Lists (ACLs) on interfaces that should accept H.323 traffic. This may greatly reduce exposure until an upgrade can be performed. • Revisit this site for updated information concerning this vulnerability. • See update section below.

The following products that utilize the H323 protocol have been found to be unaffected by the OUSPG tool.

Avaya Products	**Version**	**Status**
46xx Series IP Telephones	Firmware Versions 1.5 and later	Not Affected
Communication Manager API	R1.3 and later	Not Affected
Interactive Response	R1.0 and later	Not Affected
IP Agent	V1.0 and later	Not Affected
IP Softphone	R1.0 and later	Not Affected
IP Softphone for Pocket PC	R1.0 and later	Not Affected
Modular Messaging	R1.0 and R1.1	Not Affected
Speech Access for Communication Manager	V1.0	Not Affected

As additional information is known, this advisory will be updated.

Update (March 30, 2004)

Communication Manager Servers S8700, S8500, S8300, S8100, DEFINITY Server R, and DEFINITY Server SI/CSI

Software Update Status

DEFINITY Server R & DEFINITY Server CSI/SI

R9 & R10 customers may address the vulnerability by upgrading to the R10 field load 50 (R010r.01.0.050.0 or R010i.01.0.050.0). This load is now available as a field trial

load and can be obtained by contacting the Technical Services Organization (TSO) at 1 (800) 242-2121.

Communication Manager 1.1 through 1.3.1 customers may address the vulnerability by upgrading to the 1.3.1 field load 535 (R011r.03.1.535.0 or R011i.03.1.535.0). This load is now available and can be obtained by contacting the TSO at 1 (800) 242-2121.

Communication Manager 2.0 customers may address the vulnerability by upgrading to 2.0.1, which became available on February 9, 2004 (CSI/SI only - the R isn't available on CM 2.0 or CM 2.0.1). There will be a Product Correction Notice (PCN) that can be used to upgrade.

IP600 & DEFINITY One & S8100

R9 customers should contact the TSO for a patch. R9.5.3 will also address this issue and will be available via a hard drive upgrade on April 5th via PCN 1438B.

R10 through CM 2.0 customers may address the vulnerability by upgrading to Communication Manager 2.0.1, which became available on February 9, 2004. PCN 1417B to upgrade to 2.0.1 is now available.

S8300, S8500, & S8700 Media Servers

Communication Manager 1.1 through 1.3.1 customers may address the vulnerability by installing a new software update (super-patch) or upgrade to the 1.3.1 field load 535 (R011x.03.1.535.0). Software update 03.1.531.0-6561 is now available on via the Support website. The field load is now available through the TSO by calling 1-800-242-2121.

Customers running Communication Manager 2.0 on S8500 and S8700 Media Servers may address the vulnerability by upgrading to 2.0.1, which became available on February 9, 2004. There will be a Product Correction Notice (PCN) that can be used to upgrade.

Customers running Communication Manager 2.0 or 2.0.1 on the S8300 Media Server may address the vulnerability by upgrading to 2.0.1 field load 222 or later, or installing a patch available from the TSO. This field load is now available and can be obtained by contacting the TSO at 1 (800) 242-2121. The patch is also now available and can be obtained by contacting the TSO at 1 (800) 242-2121.

Additional Information: Additional information may be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative.

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 - January 13, 2004 - Initial statement issued.

V 1.1 - January 15, 2004 - Initial update of unaffected products.

V 1.2 - January 16, 2004 - Included SG, Softphone for PocketPC.

V 1.3 - January 21, 2004 - Included Communication Manager Servers, updated IP Softphone, IP Agent version numbers.

V 1.4 - February 3, 2004 - Added software update information for communication manager servers, moved recommended actions from update section to product table.

V 1.5 - February 20, 2004 -Indicated that R10 field load 50 (R010r.01.0.050.0 or R010i.01.0.050.0) is now available as field trial load, and that 2.0.1 became available on February 9, 2004.

V 1.6 - March 30, 2004 - Modified the software update section to identify the availability of field loads and patches.

V 2.0 - July 26, 2004 - Updated advisory to state VPNos 4.4 was released in February 04.

See http://support.avaya.com/security for the latest status of this 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.