Software Engineering Institute
Carnegie Mellon University

2004 CERT Advisories

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 CA-2004-01: Multiple H.323 Message Vulnerabilities

Original release date: January 13, 2004
Last revised: April 05, 2004
Source: CERT/CC, NISCC

A complete revision history can be found at the end of this file.

Systems Affected

- Many software and hardware systems that implement the H.323 protocol
  Examples include
  - Voice over Internet Protocol (VoIP) devices and software
  - Video conferencing equipment and software
  - Session Initiation Protocol (SIP) devices and software
  - Media Gateway Control Protocol (MGCP) devices and software
  - Other networking equipment that may process H.323 traffic (e.g., routers and firewalls)

Overview

A number of vulnerabilities have been discovered in various implementations of the multimedia telephony protocol H.323. Voice over Internet Protocol (VoIP) and video conferencing equipment and software can use these protocols to communicate over a variety of computer networks.

I. Description

The U.K. National Infrastructure Security Co-ordination Centre (NISCC) has reported multiple vulnerabilities in different vendor implementations of the multimedia telephony protocol H.323. H.323 is an international standard protocol, published by the International Telecommunications Union, used to facilitate communication among telephony and multimedia systems. Examples of such systems include VoIP, video-conferencing equipment, and network devices that manage H.323 traffic. A test suite developed by NISCC and the University of Oulu Security Programming Group (OUSPG) has exposed multiple vulnerabilities in a variety of implementations of the H.323 protocol (specifically its connection setup sub-protocol H.225.0).

Information about individual vendor H.323 implementations is available in the Vendor Information section below, and in the Vendor Information section of NISCC Vulnerability Advisory 006489/H323.

The U.K. National Infrastructure Security Co-ordination Centre is tracking these vulnerabilities as NISCC/006489/H.323. The CERT/CC is tracking this issue as VU#749342. This reference number corresponds to CVE candidate CAN-2003-0819, as referenced in Microsoft Security Bulletin MS04-001.

II. Impact

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.

III. Solution

Apply a patch or upgrade

Appendix A and the **Systems Affected** section of Vulnerability Note VU#749342 contain information provided by vendors for this advisory. However, as vendors report new information to the CERT/CC, we will only update VU#749342. If a particular vendor is not listed, we have not received their comments. Please contact your vendor directly.

Filter network traffic

Sites are encouraged to apply network packet filters to block access to the H.323 services at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be filtered include

- 1720/TCP
- 1720/UDP

Note these are default ports only and may vary on a site-by-site basis.

If access cannot be filtered at the network perimeter, the CERT/CC recommends limiting access to only those external hosts that require H.323 for normal operation. As a general rule, filtering **all** types of network traffic that are not required for normal operation is recommended.

It is important to note that some firewalls process H.323 packets and may themselves be vulnerable to attack. As noted in some vendor recommendations like Cisco Security Advisory 20040113-h323 and Microsoft Security Bulletin MS04-001, certain sites may actually want to *disable* application layer inspection of H.323 network packets.

Protecting your infrastructure against these vulnerabilities may require careful coordination among application, computer, network, and telephony administrators. You may have to make tradeoffs between security and functionality until vulnerable products can be updated. For example, blocking port 1720/udp on segments of a network may break certain functionality related to gateway discovery..

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. Please see the **Systems Affected** section of Vulnerability Note VU#749342 and the **Vendor Information** section of NISCC Vulnerability Advisory 006489/H323 for the latest information regarding the response of the vendor community to this issue.

3Com

No statement is currently available from the vendor regarding this vulnerability.

Alcatel

No statement is currently available from the vendor regarding this vulnerability.

Apple Computer Inc.

Apple: Not Vulnerable. Mac OS X and Mac OS X Server do not contain the issue described in this note.

AT&T

No statement is currently available from the vendor regarding this vulnerability.

Avaya

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uni-ras.gov.uk/vuls/2004/006489/h323.htm

Borderware

No statement is currently available from the vendor regarding this vulnerability.

Check Point

No statement is currently available from the vendor regarding this vulnerability.

BSDI

No statement is currently available from the vendor regarding this vulnerability.

Cisco Systems Inc.

Please see http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

Clavister

No statement is currently available from the vendor regarding this vulnerability.

Computer Associates

No statement is currently available from the vendor regarding this vulnerability.

Cyberguard

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uni-ras.gov.uk/vuls/2004/006489/h323.htm

Debian

No statement is currently available from the vendor regarding this vulnerability.

D-Link Systems

No statement is currently available from the vendor regarding this vulnerability.

Conectiva

No statement is currently available from the vendor regarding this vulnerability.

EMC Corporation

No statement is currently available from the vendor regarding this vulnerability.

Engarde

No statement is currently available from the vendor regarding this vulnerability.

eSoft

We don't have an H.323 implementation and thus aren't affected by this.

Extreme Networks

No statement is currently available from the vendor regarding this vulnerability.

F5 Networks

No statement is currently available from the vendor regarding this vulnerability.

Foundry Networks Inc.

No statement is currently available from the vendor regarding this vulnerability.

FreeBSD

No statement is currently available from the vendor regarding this vulnerability.

Fujitsu

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Global Technology Associates

No statement is currently available from the vendor regarding this vulnerability.

Hitachi

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Hewlett-Packard Company

Vulnerable

Please also see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Ingrian Networks

No statement is currently available from the vendor regarding this vulnerability.

Intel

No statement is currently available from the vendor regarding this vulnerability.

Intoto

No statement is currently available from the vendor regarding this vulnerability.

Juniper Networks

No statement is currently available from the vendor regarding this vulnerability.

Lachman

No statement is currently available from the vendor regarding this vulnerability.

Linksys

No statement is currently available from the vendor regarding this vulnerability.

Lotus Software

No statement is currently available from the vendor regarding this vulnerability.

Lucent Technologies

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uni-ras.gov.uk/vuls/2004/006489/h323.htm

Microsoft Corporation

Please see http://www.microsoft.com/technet/security/bulletin/MS04-001.asp

MontaVista Software

No statement is currently available from the vendor regarding this vulnerability.

MandrakeSoft

No statement is currently available from the vendor regarding this vulnerability.

Multi-Tech Systems Inc.

No statement is currently available from the vendor regarding this vulnerability.

NEC Corporation

No statement is currently available from the vendor regarding this vulnerability.

NetBSD

NetBSD does not ship any H.323 implementations as part of the Operating System.

There are a number of third-party implementations available in the pkgsrc system. As these products are found to be vulnerable, or updated, the packages will be updated accordingly. The audit-packages mechanism can be used to check for known-vulnerable package versions.

Netfilter

No statement is currently available from the vendor regarding this vulnerability.

NetScreen

No statement is currently available from the vendor regarding this vulnerability.

Network Appliance

No statement is currently available from the vendor regarding this vulnerability.

Nokia

No statement is currently available from the vendor regarding this vulnerability.

Nortel Networks

The following Nortel Networks Generally Available products and solutions are potentially affected by the vulnerabilities identified in NISCC Vulnerability Advisory 006489/H323 and CERT VU#749342:

Business Communications Manager (BCM) (all versions) is potentially affected; more information is available in Product Advisory Alert No. PAA 2003-0392-Global.

Succession 1000 IP Trunk and IP Peer Networking, and 802.11 Wireless IP Gateway are potentially affected; more information is available in Product Advisory Alert No. PAA-2003-0465-Global.

For more information please contact

North America: 1-800-4NORTEL or 1-800-466-7835
Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at
http://www.nortelnetworks.com/help/contact/global/

Or visit the eService portal at http://www.nortelnetworks.com/cs
under *Advanced Search*.

If you are a channel partner, more information can be found under http://www.nortelnetworks.com/pic under *Advanced Search*.

Novell

No statement is currently available from the vendor regarding this vulnerability.

Objective Systems Inc.

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

OpenBSD

No statement is currently available from the vendor regarding this vulnerability.

Openwall GNU/*/Linux

No statement is currently available from the vendor regarding this vulnerability.

RadVision

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Red Hat Inc.

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Oracle Corporation

No statement is currently available from the vendor regarding this vulnerability.

Riverstone Networks

No statement is currently available from the vendor regarding this vulnerability.

Secure Computing Corporation

No statement is currently available from the vendor regarding this vulnerability.

SecureWorks

No statement is currently available from the vendor regarding this vulnerability.

Sequent

No statement is currently available from the vendor regarding this vulnerability.

Sony Corporation

No statement is currently available from the vendor regarding this vulnerability.

Stonesoft

No statement is currently available from the vendor regarding this vulnerability.

Sun Microsystems Inc.

Sun SNMP does not provide support for H.323, so we are not vulnerable. And so far we have not found any bundled products that are affected by this vulnerability. We are also actively investigating our unbundled products to see if they are affected. Updates will be provided to this statement as they become available.

SuSE Inc.

No statement is currently available from the vendor regarding this vulnerability.

Symantec Corporation

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Unisys

No statement is currently available from the vendor regarding this vulnerability.

TandBerg

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Tumbleweed Communications Corp.

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

TurboLinux

No statement is currently available from the vendor regarding this vulnerability.

uniGone

Please see the NISCC Vulnerability Advisory 006489/H323 at http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

WatchGuard

No statement is currently available from the vendor regarding this vulnerability.

Wirex

No statement is currently available from the vendor regarding this vulnerability.

Wind River Systems Inc.

No statement is currently available from the vendor regarding this vulnerability.

Xerox

Not Vulnerable

A response to this vulnerability is available from our Security Information site: http://www.xerox.com/security.

ZyXEL

No statement is currently available from the vendor regarding this vulnerability.

The CERT Coordination Center thanks the NISCC Vulnerability Management Team and the University of Oulu Security Programming Group (OUSPG) for coordinating the discovery and release of the technical details of this issue.

Feedback may be directed to the authors: Jeffrey S. Havrilla, Mindi J. McDowell, Shawn V. Hernan and Jason A. Rafail.

This document is available from: http://www.preview.cert.org/advisories/CA-2004-01.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Jan 13, 2004:  Initial release

Jan 15, 2004:  Added caveat to filtering workaround

Jan 15, 2004:  Updated Xerox statement

Apr 05, 2004:  Updated HP statement
```

2 CA-2004-02: Email-borne Viruses

Original release date: January 27, 2004
Last revised: --
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Any system running Microsoft Windows (all versions from Windows 95 and up) and used for reading email or accessing peer-to-peer file sharing services.

Overview

In recent weeks there have been several mass-mailing viruses released on the Internet. It is important for users to understand the risks posed by these pieces of malicious code and the steps necessary to protect their systems from virus infection.

I. Description

Over the past week, we have seen two more mass-mailing viruses, W32/Bagle and W32/Novarg, impact a significant number of home users and sites. The technology used in these viruses is not significantly different from prior mass-mailing viruses such as W32/Sobig and W32/Mimail. Unsolicited email messages containing attachments are sent to unsuspecting recipients. They may contain a return address, a provocative envelope, or something else that encourages its receiver to open it. This technique is called social engineering. Because we are trusting and curious, social engineering is often effective. The widespread impact of these latest viruses, which rely on human intervention to spread, demonstrates the effectiveness of social engineering.

It continues to be important to ensure that anti-virus software is used and updated regularly, that attachments are examined on mail servers, and that firewalls filter unneeded ports and protocols. It also remains necessary that users be educated about the dangers of opening attachments, especially executable attachments.

II. Impact

A virus infection can have significant consequences on your computer system. These consequences include, but are not limited to:

- **Information disclosure** - Mass-mailing viruses typically harvest email addresses from the address books or files found on an infected system. Some viruses will also attempt to send files from an infected host to other potential victims or even back to the virus author. These files may contain sensitive information.

- **Add/Modify/Delete files** - Once a system is compromised, a virus could potentially add, modify or delete arbitrary files on the system. These files may contain personal information or be required for the proper operation of the computer system.
- **Affect system stability** - Viruses can consume significant amounts of computer resources causing a system to run slowly or be rendered unusable.
- **Install a backdoor** - Many viruses will install a backdoor on an infected system. This backdoor may be used by a remote attacker to gain access to the system, or view/add/modify/delete files on the system. These backdoors may also be leveraged to download and control additional tools for use in distributed denial-of-service (DDoS) attacks against other sites.
- **Attack other systems** - Systems infected by viruses are frequently used to attack other systems. These attacks frequently involve attempts to exploit vulnerabilities on the remote systems or denial-of-service attacks that utilize a high volume of network traffic.
- **Send unsolicited bulk email (spam) to other users** - There have been numerous reports of spammers leveraging compromised systems to send unsolicited bulk email. Frequently these compromised systems are poorly protected end user computers (e.g., home and small business systems).

III. Solution

In addition to following the steps outlined in this section, the CERT/CC encourages home users to review the "Home Network Security" documents.

Run and maintain an anti-virus product

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first line of defense against malicious code attacks. Users may wish to read IN-2003-01 for more information on anti-virus software and security issues.

Most antivirus software vendors release frequently updated information, tools, or virus databases to help detect and recover from malicious code. Therefore, it is important that users keep their antivirus software up to date. The CERT/CC maintains a partial list of antivirus vendors.

Many antivirus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

Do not run programs of unknown origin

Do not download, install, or run a program unless you know it to be authored by a person or company that you trust.

Email users should be wary of unexpected attachments. Be sure you know the source of an attachment before opening it. Also remember that it is not enough that the mail originated from an email address you recognize. The Melissa virus spread precisely because it originated from a familiar email address.

Users should also be wary of URLs in email messages. URLs can link to malicious content that in some cases may be executed without user intervention. A common social engineering technique known as "phishing" uses misleading URLs to entice users to visit malicious web sites. These sites spoof legitimate web sites to solicit sensitive information such as passwords or account numbers.

In addition, users of Internet Relay Chat (IRC), Instant Messaging (IM), and file-sharing services should be particularly careful of following links or running software sent to them by other users. These are commonly used methods among intruders attempting to build networks of distributed denial-of-service (DDoS) agents.

Use a personal firewall

A personal firewall will not necessarily protect your system from an email-borne virus, but a properly configured personal firewall may prevent the virus from downloading additional components or launching attacks against other systems. Unfortunately, once on a system, a virus may be able to disable a software firewall, thus eliminating its protection.

Email gateway filtering

Depending on your business requirements, it is advisable to configure filtering of specific file extensions of email attachments at the email gateway. This filtering should be configured carefully, as this may affect legitimate attachments as well. It is recommended that attachments are quarantined for later examination and/or possible retrieval.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

Steps for Recovering from a UNIX or NT System Compromise

Authors: Jeff Carpenter, Chad Dougherty, Jeff Havrilla, Allen Householder, Brian King, Marty Lindner, Art Manion, Damon Morda, Rob Murawski

This document is available from: http://www.preview.cert.org/advisories/CA-2004-02.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University

Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

January 27, 2004: Initial release