Software Engineering Institute
Carnegie Mellon University

2003 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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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-2003-01: Buffer Overflows in ISC DCHPD Minires Library

Original release date: January 15, 2003
Last revised: March 26, 2003
Source: CERT/CC

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

Systems Affected

- Systems running ISC DHCPD versions 3.0 through 3.0.1RC10, inclusive.
- For detailed vendor status information, see VU#284857

Overview

The Internet Software Consortium (ISC) has discovered several buffer overflow vulnerabilities in their implementation of DHCP (ISC DHCPD). These vulnerabilities may allow remote attackers to execute arbitrary code on affected systems. At this time, we are not aware of any exploits.

I. Description

There are multiple remote buffer overflow vulnerabilities in the ISC implementation of DHCP. As described in RFC 2131, "the Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network." In addition to supplying hosts with network configuration data, ISC DHCPD allows the DHCP server to dynamically update a DNS server, eliminating the need for manual updates to the name server configuration. Support for dynamic DNS updates is provided by the NSUPDATE feature.

During an internal source code audit, developers from the ISC discovered several vulnerabilities in the error handling routines of the minires library, which is used by NSUPDATE to resolve hostnames. These vulnerabilities are stack-based buffer overflows that may be exploitable by sending a DHCP message containing a large hostname value. *Note: Although the minires library is derived from the BIND 8 resolver library, these vulnerabilities do not affect any current versions of BIND.*

The CERT/CC is tracking this issue as VU#284857. This reference number corresponds to CVE candidate CAN-2003-0026.

II. Impact

Remote attackers may be able to execute arbitrary code with the privileges of the user running ISC DHCPD.

III. Solution

Upgrade or apply a patch

The ISC has addressed these vulnerabilities in versions 3.0pl2 and 3.0.1RC11 of ISC DHCPD. If your software vendor supplies ISC DHCPD as part of an operating system distribution, please see Appendix A for vendor-specific patch information.

For a detailed list of vendors that have been notified of this issue by the CERT/CC, please see

http://www.kb.cert.org/vuls/id/284857#systems

Disable dynamic DNS updates (NSUPDATE)

As an interim measure, the ISC recommends disabling the NSUPDATE feature on affected DHCP servers.

Block external access to DHCP server ports

As an interim measure, it is possible to limit exposure to these vulnerabilities by restricting external access to affected DHCP servers on the following ports:

```
bootps 67/tcp # Bootstrap Protocol Server

bootps 67/udp # Bootstrap Protocol Server

bootpc 68/tcp # Bootstrap Protocol Client

bootpc 68/udp # Bootstrap Protocol Client
```

Disable the DHCP service

As a general rule, the CERT/CC recommends disabling any service or capability that is not explicitly required. Depending on your network configuration, you may not need to use DHCP.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Alcatel

Following CERT advisory CA-2003-01 on security vulnerabilities in the ISC DHCP implementation, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that none of our products is impacted. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential ISC DHCP security vulnerabilities and will provide updates if necessary.

Apple Computer, Inc.

Mac OS X and Mac OS X Server do not contain the vulnerability described in this notice.

Berkeley Software Design, Inc. (BSDI)

This vulnerability is addressed by the M431-001 and M500-004 patches for the 4.3.1 and 5.0 versions of BSD/OS.

Cisco Systems

No Cisco products have been found to be affected by this vulnerability.

Several Cisco products do utilize the ISC DHCPD, however, no Cisco products implement the ISC DHCPD NSUPDATE feature, nor do they include the minires library.

Cray Inc.

Cray Inc. is not vulnerable as dhcpd is not supported on any of its products.

Debian

Debian has updated their distribution with DSA 231.

For the stable distribution (woody) this problem has been fixed in version 3.0+3.0.1rc9-2.1.

The old stable distribution (potato) does not contain dhcp3 packages.

For the unstable distribution (sid) this problem has been fixed in version 3.0+3.0.1rc11-1.

Fujitsu

Fujitsu's UXP/V OS is not vulnerable because it does not support the ISC DHCPD.

Hewlett-Packard Company

```
Source: Hewlett-Packard Company

 Software Security Response Team

cross reference id: SSRT2423

 HP-UX - not vulnerable
 HP-MPE/ix - not vulnerable

 HP Tru64 UNIX - not vulnerable

 HP OpenVMS - not vulnerable

 HP NonStop Servers - not vulnerable
```

To report potential security vulnerabilities in HP software, send an E-mail message to: mailto:security-alert@hp.com.

Hitachi, Ltd.

We've checked up on our router (Hitachi,Ltd. GR2000 series) about [VU#284857]. Our DHCP implementation is NOT vulnerable.

IBM Corporation

IBM's AIX does not ship with the ISC DHCP daemon. The issues discussed in VU#284857 or any following advisories based on this vulnerability note do not pertain to AIX.

Ingrian Networks

Ingrian Networks products are not vulnerable to VU#284857.

Internet Software Consortium

We have a patched version of 3.0 available (3.0pl2) and a new release candidate for the next bugfix release (3.0.1RC11). Both of these new releases are available from http://www.isc.org/products/DHCP/.

Microsoft Corporation

Microsoft products do not use the libraries in question. Microsoft products are not affected by this vulnerability.

MontaVista Software

None of MontaVista Software's Linux products are vulnerable to this issue.

NEC Inc.

```
[Server Products]

* EWS/UP 48 Series operating system

- is NOT vulnerable.
```

NetBSD

Currently supported versions of NetBSD do not contain the error handling routine vulnerabilities. Such vulnerabilities were fixed prior to the release of NetBSD 1.5.

With respect to the patch to ns_name.c, we believe that this is good defensive programming and have applied the patch to NetBSD-current. However, all calls to ns_name_ntol in the NetBSD source base pass a correct, constant, non-zero value as the datsiz parameter.

Therefore, NetBSD is not vulnerable.

NetScreen

NetScreen is not vulnerable to this issue.

OpenBSD

OpenBSD's dhcp support is much modified, does not have that feature, and therefore does not have that bug.

Openwall GNU/*/Linux

Openwall GNU/*/Linux is not vulnerable. We don't yet provide a DHCP suite.

Red Hat Inc.

Red Hat distributes a vulnerable version of ISC DHCP in Red Hat Linux 8.0. Other distributions of Red Hat Linux are not vulnerable to these issues. New DHCP packages are available along with our advisory at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

http://rhn.redhat.com/errata/RHSA-2003-011.html

Riverstone Networks

Riverstone Networks is not vulnerable to VU#284857.

Sun Microsystems, Inc.

Sun confirms that we are not vulnerable to the issues described in VU#284857. Solaris does not ship the ISC DHCPD and does not use any of the ISC DHCPD source in its version of DHCPD.

SuSE Linux AG

We are preparing updates, that will be released soon.

Xerox

A response to this advisory is available from our web site: http://www.xerox.com/security.

The CERT Coordination Center thanks David Hankins of the Internet Software Consortium for notifying us about this problem and for helping us to construct this document. We also thank Jacques A. Vidrine for drawing attention to this issue.

Author: This document was written by Jeffrey P. Lanza.

Revision History

```
Jan 15, 2003: Initial release

Jan 20, 2003: Added vendor statement for Debian

Jan 28, 2003: Added vendor statement for Microsoft Corporation

Mar 25, 2003: Added vendor statement for Ingrian Networks

Mar 26, 2003: Updated vendor statement for Xerox Corporation

Mar 26, 2003: Added vendor statement for Alcatel
```

2 CA-2003-02: Double-Free Bug in CVS Server

Original issue date: January 22, 2003
Last revised: March 27, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running CVS Home project versions of CVS prior to 1.11.5
- Operating system distributions that provide CVS
- Source code repositories managed by CVS
- For detailed vendor status information, see VU#650937

Overview

A "double-free" vulnerability in the Concurrent Versions System (CVS) server could allow an unauthenticated, remote attacker with read-only access to execute arbitrary code, alter program operation, read sensitive information, or cause a denial of service.

I. Description

CVS is a version control and collaboration system that is widely used by open-source software development projects. CVS is commonly configured to allow public, anonymous, read-only access via the Internet.

The CVS server component contains a "double-free" vulnerability that can be triggered by a set of specially crafted directory requests. While processing these requests, an error-checking routine may attempt to `free()` the same memory reference more than once. Deallocating the already freed memory leads to heap corruption, which an attacker could leverage to execute arbitrary code, alter the logical operation of the CVS server program, or read sensitive information stored in memory. In most cases, heap corruption will result in a segmentation fault, causing a denial of service.

The CVS server process is typically started by the Internet services daemon (`inetd`) and runs with root privileges. Arbitrary code inserted by an attacker would therefore run with root privileges.

This issue is being tracked as VU#650937. This reference number corresponds to CVE candidate CAN-2002-0059. This issue was researched and reported by Stefan Esser of e-matters.

II. Impact

Depending on configuration, operating system, and platform architecture, a remote attacker with anonymous, read-only access to a vulnerable CVS server could execute arbitrary code, alter the operation of the server program, read sensitive information, or cause a denial of service. There is also a significant secondary impact. An attacker who is able to compromise a CVS server could modify source-code repositories to contain Trojan horses, backdoors, or other malicious code.

III. Solution

Apply a patch or upgrade

Apply the appropriate patch or upgrade as specified by your vendor. See Appendix A below and the Systems Affected section of VU#650937 for further information.

Disable or restrict anonymous CVS access

As a temporary solution until patches or upgrades can be applied, or to improve the security of CVS servers in the long term, consider the following workarounds and configurations:

- Disable anonymous CVS server access completely.
- Block or restrict access to CVS servers from untrusted hosts and networks. Anonymous access to CVS servers using `:cvspserver:` is typically provided on port 2401/tcp.
- Configure CVS servers to run in restricted (`chroot`) environments.
- Run CVS servers with the minimum set of privileges required on the host file system.
- Provide separate systems for development (write) and public/anonymous (read-only) CVS access.
- Host public/anonymous CVS servers on single-purpose, secured systems.

These workarounds and configurations are not complete solutions and may not prevent exploitation of this vulnerability. Other features inherent in CVS may give anonymous users the ability to gain shell access.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments. The Systems Affected section of VU#650937 contains additional vendor status information.

Conectiva

Conectiva Linux is affected by this issue and updated packages are available at ftp://atualizacoes.conectiva.com.br/:

6.0/SRPMS/cvs-1.10.8-5U60_3cl.src.rpm

6.0/RPMS/cvs-1.10.8-5U60_3cl.i386.rpm
6.0/RPMS/cvs-doc-1.10.8-5U60_3cl.i386.rpm
7.0/SRPMS/cvs-1.11-7U70_2cl.src.rpm
7.0/RPMS/cvs-1.11-7U70_2cl.i386.rpm
7.0/RPMS/cvs-doc-1.11-7U70_2cl.i386.rpm
8/SRPMS/cvs-1.11-9U80_2cl.i386.rpm
8/RPMS/cvs-1.11-9U80_2cl.i386.rpm
8/RPMS/cvs-doc-1.11-9U80_2cl.i386.rpm

An official announcement is pending and will show up in our updates website at http://distro.conectiva.com.br/atualizacoes?idioma=en shortly.

Cray Inc.

Cray Inc. supports CVS through their Cray Open Software (COS) package. COS 3.3 and earlier is vulnerable. A new CVS will be available shortly. Please contact your local Cray service representative if you need this new package.

CVS Home

CVS release 1.11.5 addresses this issue for CVS servers. CVS clients are not affected.

Debian

Debian has updated their distribution with DSA 233.
http://www.debian.org/security/2003/dsa-233

For the stable distribution (woody) this problem has been fixed in version 1.11.1p1debian-8.1.

For the old stable distribution (potato) this problem has been fixed in version 1.10.7-9.2.

For the unstable distribution (sid) this problem will be fixed soon.

Fujitsu

Fujitsu's UXP/V o.s. is not vulnerable to the problem reported in VU#650937 because it does not support CVS server.

Hewlett-Packard

SOURCE: Hewlett-Packard Company and Compaq Computer Corporation, a wholly-owned subsidiary of Hewlett-Packard Company

RE: x-reference SSRT3463

Not Vulnerable:
HP-UX
HP-MPE/ix
HP Tru64 UNIX
HP NonStop Servers
HP OpenVMS

To report any security issue for any HP software products send email to security-alert@hp.com

Hitachi

GR2000 router does not contain any parts of the CVS. Therefore, it is not vulnerable.

IBM

The AIX operating system does not ship with CVS. However, CVS is available for installation on AIX from the Linux Affinity Toolbox.

CVS versions 1.11.1p1-2 and earlier are vulnerable to the issues discussed in CERT Vulnerability Note VU#650937 and any advisories which follow.

Users are advised to download CVS 1.11.1p1-3 from:

ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/RPMS/ppc/cvs/
cvs-1.11.1p1-3.aix4.3.ppc.rpm

Please note that the above address was wrapped to two lines.

CVS 1.11.1p1-3 contains the security fixes made in CVS 1.11.5 to address these issues.

This software is offered on an "as-is" basis.

Ingrian Networks

Ingrian Networks platforms are not vulnerable to VU#650937.

NEC Corporation

Subject: VU650937

sent on January 23, 2003

[Server Products]

- EWS/UP 48 Series operating system
  - is NOT vulnerable, which does not include CVS.

NetBSD

The NetBSD project's CVS servers are constructed such that this issue exposed no vulnerability. Nevertheless the fix was applied, and incorporated into the in-tree version of CVS for the benefit of NetBSD users who may be offering their own CVS services.

Openwall GNU/*/Linux

We don't yet re-distribute CVS in Openwall GNU/*/Linux. We do, however, provide public anonymous CVS access to a copy of our repository, hosted off a separate machine and in a chroot jail. This kind of vulnerabilities in CVS was expected, and our anoncvs setup is mostly resistant to them: read-only access to the repository is achieved primarily with the use of regular Unix permissions, not controls built into CVS. CVS LockDir option is used to direct CVS lock files to a separate directory tree, actually writable to the pseudo-user. Nevertheless, the anoncvs server has been upgraded to CVS 1.11.5 a few hours after it was released.

Red Hat, Inc.

Red Hat Linux and Red Hat Linux Advanced Server shipped with a cvs package vulnerable to these issues. New cvs packages are now available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Linux Advanced Server:

http://rhn.redhat.com/errata/RHSA-2003-013.html

Red Hat Linux:

http://rhn.redhat.com/errata/RHSA-2003-012.html

Sun Microsystems Inc.

Sun does not include CVS with Solaris and therefore Solaris is not affected by this issue. Sun does provide CVS on the Solaris Companion CD:

http://wwws.sun.com/software/solaris/freeware/index.html

as an unsupported package which installs to /opt/sfw and is vulnerable to this issue. Sites using the freeware version of CVS from the Solaris Companion CD will have to upgrade to a later version from CVS Home.

Sun Linux, versions 5.0.3 and below, does ship with a vulnerable CVS package. Sun recommends that CVS services be disabled on affected Sun Linux systems until patches are available for this issue.

Sun will be publishing a Sun Alert for Sun Linux describing the patch information which will be available from: http://sunsolve.Sun.COM

Appendix B References

- CERT/CC Vulnerability Note VU#650937 - http://www.kb.cert.org/vuls/id/650937
- e-matters Advisory 01/2003 - http://security.e-matters.de/advisories/012003.html

This vulnerability was reported by Stefan Esser of e-matters.

Author: Art Manion.

Revision History

January 22, 2003: Initial release

January 23, 2003: Fixed Red Hat advisory URL

February 4, 2003: Updated Sun statement, added Fujitsu, Hitachi, NEC, and NetBSD statements

February 14, 2003: Added Ingrian statement

March 27, 2003: Updated Solution section

3 CA-2003-03: Buffer Overflow in Windows Locator Service

Original issue date: January 23, 2003
Last revised: January 24, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0, Terminal Server Edition
- Microsoft Windows 2000
- Microsoft Windows XP

Overview

A buffer overflow vulnerability in the Microsoft Windows Locator service could allow a remote attacker to execute arbitrary code or cause the Windows Locator service to fail. This service is enabled and running by default on Windows 2000 domain controllers and Windows NT 4.0 domain controllers.

I. Description

A buffer overflow in the Windows Locator service may make it possible for a remote attacker to execute arbitrary code on a vulnerable system by sending an overly large request to the Windows Locator service. Microsoft describes the Windows Locator service as "a name service that maps logical names to network-specific names." From MS03-001:

A client that is going to make a Remote Procedure Call (RPC) can call the Locator service to resolve a logical name for a network object to a network-specific name for use in the RPC. For example, if a print server has the logical name "laserprinter", an RPC client could call the Locator service to find out the network-specific name that mapped to "laserprinter". The RPC client uses the network-specific name when it makes the RPC call to the service.

Further information about this vulnerability can be found in Microsoft Security Bulletin MS03-001 and in CERT/CC Vulnerability Note VU#610986, which correspond to CVE candidate CAN-2003-0003.

II. Impact

A remote attacker may be able to execute arbitrary code on a vulnerable system, or cause the Windows Locator service to fail. An attacker who is able to compromise a domain controller might be able to cause the compromised domain controller to trust the attacker's domain.

III. Solution

Apply a patch

Microsoft has provided the following information (contained within MS03-001) to assist you in downloading the appropriate patch for your platform(s):

- Windows NT 4.0:
  - All except Japanese NEC and Chinese - Hong Kong
  - Japanese NEC
  - Chinese - Hong Kong
- Windows NT 4.0, Terminal Server Edition:
  - All
- Windows 2000:
  - All except Japanese NEC
  - Japanese NEC
- Windows XP:
  - 32-bit Edition
  - 64-bit Edition

Disable vulnerable service

Until a patch can be applied, you may wish to disable the Windows Locator service. To determine if the Windows Locator service is running, Microsoft recommends the following:

- *The status of the "Remote Procedure Call (RPC) Locator" service and how it is started (automatically or manually) can be viewed in the Control Panel. For Windows 2000 and Windows XP, use Control Panel | Administrative Tools | Services, and on Windows NT 4.0, use Control Panel | Services.*
- *It is also possible to determine the status of the Locator service from the command line by entering:* **net start**
- *A list of services will be displayed. If "Remote Procedure Call (RPC) Locator" appears in the list, then the locator service is running.*

To disable the Windows Locator service, Microsoft recommends the following:

- *An administrator can disable the Locator service by setting the RpcLocator service status to "disabled" in the services control panel.*
- *The service can also be stopped via the command line using the sc.exe program, which ships with Windows XP and is included as part of the Windows 2000 Resource Kit. The following command will stop the service*: **sc stop RpcLocator**
- *To disable the service using the command line tool, use the following:* **sc config RpcLocator start= disabled**

Restrict access to NetBIOS

You may wish to block access to NetBIOS from outside your network perimeter, specifically by blocking access to ports 139/TCP and 445/TCP. This will limit your exposure to attacks. However, blocking at the network perimeter would still allow attackers within the perimeter of your network to exploit the vulnerability. It is important to understand your network's configuration and service requirements before deciding what changes are appropriate.

As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. Before deciding to disable the Windows Locator service, carefully consider your service requirements.

Please also note that Microsoft is actively deploying the patches for this vulnerability via Windows Update.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft Corporation

Please see Microsoft Security Bulletin MS03-001.

Appendix B References

- Microsoft Security Bulletin MS03-001 - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-001.asp
- CERT/CC Vulnerability Note VU#10986 - http://www.kb.cert.org/vuls/id/610986

This vulnerability was discovered by David Litchfield of Next Generation Security Software Ltd and was first described in MS03-001.

Author: Ian A. Finlay.

Revision History

January 23, 2003: Initial release

January 24, 2003: Added information about which port nubmers to block

4 CA-2003-04: MS-SQL Server Worm

Original release date: January 25, 2003
Last revised: January 27, 2003
Source: CERT/CC

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

Systems Affected

- Microsoft SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000

Overview

The CERT/CC has received reports of self-propagating malicious code that exploits a vulnerability in the Resolution Service of Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000. This worm is being referred to as the SQLSlammer, W32.Slammer, and Sapphire worm. The propagation of this malicious code has caused varied levels of network degradation across the Internet and the compromise of vulnerable machines.

I. Description

The worm targeting SQL Server computers is self-propagating malicious code that exploits the vulnerability described in VU#484891 (CAN-2002-0649). This vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow.

Once the worm compromises a machine, it will try to propagate itself. The worm will craft packets of 376-bytes and send them to randomly chosen IP addresses on port 1434/udp. If the packet is sent to a vulnerable machine, this victim machine will become infected and will also begin to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no other payload.

Activity of this worm is readily identifiable on a network by the presence of 376-byte UDP packets. These packets will appear to be originating from seemingly random IP addresses and destined for port 1434/udp.

II. Impact

Compromise by the worm confirms a system is vulnerable to allowing a remote attacker to execute arbitrary code as the local SYSTEM user. It may be possible for an attacker to subsequently leverage a local privilege escalation exploit in order to gain Administrator access to the victim system.

The high volume of 1434/udp traffic generated by hosts infected with the worm trying to find and compromise other SQL Server computers may itself lead to performance issues (including possible denial-of-service conditions) for Internet-connected hosts or for those computers on networks with compromise hosts.

III. Solution

Apply a patch

Administrators of all systems running Microsoft SQL Server 2000 and MSDE 2000 are encouraged to review CA-2002-22 and VU#484891. For detailed vendor recommendations regarding installing the patch see http://www.microsoft.com/technet/security/virus/alerts/slammer.asp.

SQL Server 2000 and MSDE 2000 both have the vulnerability documented in VU#484891. However, the propagation of the worm requires a process listening on port 1434/udp to exploit this vulnerability. This precondition is obviously present in SQL Server 2000. However, not all applications using MSDE 2000 listen to the network by default. Therefore, only certain MSDE 2000-enabled applications may be vulnerable.

Ingress/egress filtering

The following steps are only effective in limiting the damage that can be done by systems already infected with the worm. They provide no protection against the initial infection of systems. As a result, these steps are only recommended **in addition to** the preventative steps outlined above.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound traffic from the public Internet. In the network usage policy of many sites, external hosts are only permitted to initiate inbound traffic to machines that provide public services on specific ports. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services.

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet.

In the case of this worm, employing ingress and egress filtering can help prevent compromised systems on your network from attacking systems elsewhere. Blocking UDP datagrams with both source or destination ports 1434 from entering or leaving your network reduces the risk of external infected systems communicating with infected hosts inside your network.

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

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#35663]".

Feedback can be directed to the author: Roman Danyliw

This document is available from: http://www.cert.org/advisories/CA-2003-04.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/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

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

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

```
January 25, 2003: Initial release

January 26, 2003: Updated VU# information, packet size, MS Advisory
link

January 27, 2003: MSDE 2000
```

5 CA-2003-05: Multiple Vulnerabilities in Oracle Servers

Original release date: February 19, 2003
Last revised: Fri Feb 21 15:39:12 EST 2003
Source: CERT/CC

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

Systems Affected

- Systems running Oracle9i Database (Release 1 and 2)
- Systems running Oracle8i Database v 8.1.7
- Systems running Oracle8 Database v 8.0.6
- Systems running Oracle9i Application Server (Release 9.0.2 and 9.0.3)

Overview

Multiple vulnerabilities exist in Oracle software that may lead to execution of arbitrary code; the ability to read, modify, or delete information stored in underlying Oracle databases; or denial of service. All of these vulnerabilites were discovered by Next Generation Security Software Ltd.

I. Description

Multiple vulnerabilities exist in Oracle software products. The majority of these vulnerabilities are buffer overflows.

Oracle has published Security Alerts describing these vulnerabilities. If you use Oracle products listed in the "Systems Affected" section of this document, we strongly encourage you to review the following Oracle Security Alerts and apply patches as appropriate:

- Buffer Overflow in DIRECTORY parameter of Oracle9i Database Server
  http://otn.oracle.com/deploy/security/pdf/2003alert48.pdf
- Buffer Overflow in TZ_OFFSET function of Oracle9i Database Server
  http://otn.oracle.com/deploy/security/pdf/2003alert49.pdf
- Buffer Overflow in TO_TIMESTAMP_TZ function of Oracle9i Database Server
  http://otn.oracle.com/deploy/security/pdf/2003alert50.pdf
- Buffer Overflow in ORACLE.EXE binary of Oracle9i Database Server
  http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf
- Two Vulnerabilities in Oracle9i Application Server
  http://otn.oracle.com/deploy/security/pdf/2003alert52.pdf

NGSSoftware Insight Security Research Advisories describing these issues are listed below:

- Oracle9i Application Server Format String Vulnerability
  http://www.nextgenss.com/advisories/ora-appservfmtst.txt

- Oracle TO_TIMESTAMP_TZ Remote System Buffer Overrun
  http://www.nextgenss.com/advisories/ora-tmstmpbo.txt
- ORACLE bfilename function buffer overflow vulnerability
  http://www.nextgenss.com/advisories/ora-bfilebo.txt
- Oracle TZ_OFFSET Remote System Buffer Overrun
  http://www.nextgenss.com/advisories/ora-tzofstbo.txt
- Oracle unauthenticated remote system compromise
  http://www.nextgenss.com/advisories/ora-unauthrm.txt

The CERT/CC has published vulnerability notes for each of these issues as well. The vulnerability in Oracle's mod_dav module (VU#849993) has been as assigned CVE ID CAN-2002-0842.

II. Impact

Depending on the vulnerability being exploited, an attacker may be able to execute arbitrary code; read, modify, or delete information stored in underlying Oracle databases; or cause a denial of service. The vulnerabilities in "ORACLE.EXE" (VU#953746) and the WebDAV modules (VU#849993, VU#511194) may be exploited prior to authentication.

III. Solution

Apply a patch

Solutions for specific vulnerabilities can be found in the above referenced Oracle Security Alerts, NGSSoftware Insight Security Research Advisories, and individual CERT/CC Vulnerability Notes.

Mitigation Strategies

Until a patch can be applied, the CERT/CC recommends that vulnerable sites

- disable unnecessary Oracle services
- run Oracle services with the least privilege
- restrict network access to Oracle services

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Oracle Corporation

Please see the following Oracle Security Alerts:

- http://otn.oracle.com/deploy/security/pdf/2003alert48.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert49.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert50.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert52.pdf

Appendix B Reference

- http://otn.oracle.com/deploy/security/pdf/2003alert48.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert49.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert50.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf
- http://otn.oracle.com/deploy/security/pdf/2003alert52.pdf
- http://www.nextgenss.com/advisories/ora-appservfmtst.txt
- http://www.nextgenss.com/advisories/ora-tmstmpbo.txt
- http://www.nextgenss.com/advisories/ora-bfilebo.txt
- http://www.nextgenss.com/advisories/ora-tzofstbo.txt
- http://www.nextgenss.com/advisories/ora-unauthrm.txt
- http://www.kb.cert.org/vuls/id/743954
- http://www.kb.cert.org/vuls/id/953746
- http://www.kb.cert.org/vuls/id/663786
- http://www.kb.cert.org/vuls/id/840666
- http://www.kb.cert.org/vuls/id/511194
- http://www.kb.cert.org/vuls/id/849993
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0842

The CERT/CC acknowledges both Next Generation Security Software Ltd. and Oracle for providing information upon which this document is based.

Feedback can be directed to the author: Ian A. Finlay.

This document is available from: http://www.cert.org/advisories/CA-2003-05.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/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

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

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

```
February 19, 2003: Initial release

February 21, 2003: Revised description
```

6 CA-2003-06: Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)

Original release date: February 21, 2003
Last revised: Tue May 21 16:12:47 EST 2003
Source: CERT/CC

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

Systems Affected

SIP-enabled products from a wide variety of vendors are affected. Other systems making use of SIP may also be vulnerable but were not specifically tested. Not all SIP implementations are affected. See Vendor Information for details from vendors who have provided feedback for this advisory.

In addition to the vendors who provided feedback for this advisory, a list of vendors whom CERT/CC contacted regarding these problems is available from VU#528719.

Overview

Numerous vulnerabilities have been reported in multiple vendors' implementations of the Session Initiation Protocol. These vulnerabilities may allow an attacker to gain unauthorized privileged access, cause denial-of-service attacks, or cause unstable system behavior. If your site uses SIP-enabled products in any capacity, the CERT/CC encourages you to read this advisory and follow the advice provided in the Solution section below.

I. Description

The Session Initiation Protocol (SIP) is a developing and newly deployed protocol that is commonly used in Voice over IP (VoIP), Internet telephony, instant messaging, and various other applications. SIP is a text-based protocol for initiating communication and data sessions between users.

The Oulu University Secure Programming Group (OUSPG) previously conducted research into vulnerabilities in LDAP, culminating in CERT Advisory CA-2001-18, and SNMP, resulting in CERT Advisory CA-2002-03.

OUSPG's most recent research focused on a subset of SIP related to the INVITE message, which SIP agents and proxies are required to accept in order to set up sessions. By applying the PROTOS c07-sip test suite to a variety of popular SIP-enabled products, the OUSPG discovered impacts ranging from unexpected system behavior and denial of services to remote code execution. Note that "throttling" is an expected behavior.

Specifications for the Session Initiation Protocol are available in RFC3261:

http://www.ietf.org/rfc/rfc3261.txt

OUSPG has established the following site with detailed documentation regarding SIP and the implementation test results from the test suite:

http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/

The IETF Charter page for SIP is available at

http://www.ietf.org/html.charters/sip-charter.html

II. Impact

Exploitation of these vulnerabilities may result in denial-of-service conditions, service interruptions, and in some cases may allow an attacker to gain unauthorized access to the affected device. Specific impacts will vary from product to product.

III. Solution

Many of the mitigation steps recommended below may have significant impact on your everyday network operations and/or network architecture. Ensure that any changes made based on the following recommendations will not unacceptably affect your ongoing network operations capability.

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. Please consult this appendix and VU#528719 to determine if your product is vulnerable. If a statement is unavailable, you may need to contact your vendor directly.

Disable the SIP-enabled devices and services

As a general rule, the CERT/CC recommends disabling any service or capability that is not explicitly required. Some of the affected products may rely on SIP to be functional. You should carefully consider the impact of blocking services that you may be using.

Ingress filtering

As a temporary measure, it may be possible to limit the scope of these vulnerabilities by blocking access to SIP devices and services at the network perimeter.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound traffic from the public

Internet. Note that most SIP User Agents (including IP phones or "client" software) consist of a User Agent Client and a User Agent Server. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound traffic to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services. For SIP, ingress filtering of the following ports can prevent attackers outside of your network from accessing vulnerable devices in the local network that are not explicitly authorized to provide public SIP services:

```
sip 5060/udp # Session Initiation Protocol (SIP)
sip 5060/tcp # Session Initiation Protocol (SIP)
sip 5061/tcp # Session Initiation Protocol (SIP) over TLS
```

Careful consideration should be given to addresses of the types mentioned above by sites planning for packet filtering as part of their mitigation strategy for these vulnerabilities.

Please note that this workaround may not protect vulnerable devices from internal attacks.

Egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound traffic to the Internet. In the case of the SIP vulnerabilities, employing egress filtering on the ports listed above at your network border may prevent your network from being used as a source for attacks on other sites.

Block SIP requests directed to broadcast addresses at your router.

Since SIP requests can be transmitted via UDP, broadcast attacks are possible. One solution to prevent your site from being used as an intermediary in an attack is to block SIP requests directed to broadcast addresses at your router.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Alcatel

Following CERT advisory CA-2003-06 on security vulnerabilities in SIP implementations, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that the OmniPCX Enterprise 5.0 Lx is impacted. Alcatel is currently working on a fix that will be made available via our business partners. Customers may wish to contact their support for more information. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential SIP security vulnerabilities and will provide updates if necessary.

America Online Inc

Not vulnerable.

Apple Computer Inc.

There are currently no applications shipped by Apple with Mac OS X or Mac OS X Server which make use of the Session Initiation Protocol.

Avaya

Avaya products are not vulnerable.

Borderware

No BorderWare products make use of SIP and thus no BorderWare products are affected by this vulnerability.

Check Point

No Check Point products are vulnerable to the described attacks. FireWall-1 blocks the majority of the attacks described in this advisory through strict enforcement of the SIP protocol.

Cirpack

Cirpack Switches <http://www.cirpack.com/products> deployed by telecom service providers for carrier-class SIP voice services are not vulnerable to problem described in VU#528719 as of software version = 4.3c. If your Cirpack switches use earlier software version, please contact your Cirpack account manager.

Cisco Systems

Cisco Systems is addressing the vulnerabilities identified by VU#528719 across its entire product line. Cisco has released an advisory:

http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml

Clavister

No Clavister products currently incorporate support for the SIP protocol suite, and as such, are not vulnerable.

We would however like to extend our thanks to the OUSPG for their work as well as for the responsible manner in which they handle their discoveries. Their detailed reports and test suites are certainly well-received.

We would also like to reiterate the fact that SIP has yet to mature, protocol-wise as well as implementation-wise. We do not recommend that our customers set up SIP relays in parallel to our firewall products to pass SIP-based applications in or out of networks where security is a concern of note.

Columbia SIP User Agent (sipc)

Sipc (version 1.74) contains vulnerabilities identified by OUSPG PROTOS SIP Test Suite. The vulnerabilities have been resolved in sipc (version 2.0, build 2003-02-21). Please see sipc (version 1.74) vulnerabilities found by PROTOS SIP Test Suite for detailed information. We strongly advice to upgrade to sipc version 2.0, which is much more stable, has much better user interface and can perform more functions.

Dynamicsoft Inc.

Please see http://www.dynamicsoft.com/support/advisory/ca-2003-06.php.

F5 Networks

F5 Networks does not have a SIP server product, and is therefore not affected by this vulnerability.

Foundry Networks, Inc.

Foundry Networks, Inc. products do not use the SIP protocol and is not affected by the vulnerabilities described in CA-2003-06.

Fujitsu

With regards to VU#528719, Fujitsu's UXP/V o.s. is not vulnerable because the relevant function is not supported under UXP/V.

Hewlett-Packard Company

Source:
Hewlett-Packard Company

Software Security Response Team

cross reference id: SSRT2402

HP-UX - not vulnerable
HP-MPE/ix - not vulnerable
HP Tru64 UNIX - not vulnerable
HP OpenVMS - not vulnerable
HP NonStop Servers - not vulnerable

To report potential security vulnerabilities in HP software, send an E-mail message to: mailto:security-alert@hp.com

Hotsip AB

Hotsip has investigated the issues reported in VU#528719 and found that Hotsip Active Contacts(tm) PC 3.x, SIP Application Server 3.x and Presence Engine 2.x are not affected by this.

Hughes Software Systems

SIP Core stack - Not Vulnerable [Version : 5.0.1] SIP User Agent - Not Vulnerable [Version : 2.0] microSIP stack - Not Vulnerable [Version: 2.0] microUser Agent - Not Vulnerable [Version: 2.0]

IBM

SIP is not implemented as part of the AIX operating system.

The issues discussed in VU#528719 do not pertain to AIX.

IBM zSeries

zSeries customers should feel free to contact servsec@us.ibm.com with any CERT related security questions or concerns.

Indigo Software

Indigo Software certifies that its Indigo SIP Foundation Class, Indigo SIP Server & SDK and Indigo Communications Server & SDK products are NOT VULNERABLE to DoS and other attacks simulated by the PROTOS Vulnerability Assessment Test Suite. For more information, please refer to http://www.indigosw.com/html/cert_advisory.htm

Ingate Systems

Ingate Firewall and Ingate SIParator running versions prior to 3.1.3 are vulnerable to problems exposed by the PROTOS c07-sip test suite. The vulnerabilities have been fixed in version 3.1.3, which is available for download from http://www.ingate.com/upgrades/. We strongly advice to upgrade to version 3.1.3.

Intoto

Intoto, Inc has examined its SIP based product iGateway-VoIP Ver 1.0.1, for possible buffer overflow vulnerabilities documented in VU#528719, and found that iGateway-VoIP is not vulnerable to these attacks.

IP Filter

IPFilter does not do any SIP specific protocol handling and is therefore not affected by the issues mentioned in the paper cited.

IPTel

All versions of SIP Express Router up to 0.8.9 are sadly vulnerable to the OUSPG test suite. We strongly advice to upgrade to version 0.8.10. Please also apply the patch to version 0.8.10 from http://www.iptel.org/ser/security/ before installation and keep on watching this site in the future. We apologize to our users for the trouble.

Juniper Networks

Juniper Networks products are not SIP-aware, and neither generate, process, nor act as a proxy for SIP protocol messages. Therefore, Juniper Networks products are not susceptible to this vulnerability.

Customers wishing to use the packet filtering features of Juniper Networks products to block SIP protocol messages can visit the Juniper Networks product support web-site at https://www.juniper.net/support/csc/ or they can contact Juniper's Technical Assistance Center by telephone at at 1-888-314-JTAC (U.S. customers only; non-U.S. customers should call JTAC at +1 408-745-9500.)

Lucent

No Lucent products are known to be affected by this vulnerability, however we are still researching the issue and will update this statement as needed.

Mediatrix Telecom, Inc.

Tests developed by the University of Oulu and performed by Mediatrix Telecom Inc on Mediatrix VoIP Access Devices and Gateways have uncovered vulnerabilities, as per CERT vulnerability note VU#52789, that will be eliminated through software patches with the following availabilities:

- By March 21 for Mediatrix units running the SIPv2.4 firmware.
- By April 11 for Mediatrix units running the SIPv4.3 firmware.

Additional information on Mediatrix Telecom Inc products are available at www.mediatrix.com

Microsoft Corporation

Microsoft has investigated these issues. The Microsoft SIP client implementation is not affected.

NEC Corporation

===
NEC vendor statement for VU#528719
===

sent on May 20, 2003

[Server Products]

- EWS/UP 48 Series operating system
    - is NOT vulnerable, because it does not support SIP.

[Router Products]

- IX 1000 / 2000 / 5000 Series
    - is NOT vulnerable, because it does not support SIP.

[Other Network products]

- CX6820 Call Service Server Series (CA/SS/MD) V2.2
    - is NOT vulnerable.
- CX7620-VG Media Server
    - is NOT vulnerable.
- We continue to check our products which support SIP protocol.

===

NETBSD

NetBSD does not ship any implementation of SIP.

NETfilter.org

As the linux 2.4/2.5 netfilter implementation currently doesn't support connection tracking or NAT for the SIP protocol suite, we are not vulnerable to this bug.

NetScreen

NetScreen is not vulnerable to this issue.

Network Appliance

NetApp products are not affected by this vulnerability.

Nokia

Nokia IP Security Platforms based on IPSO, Nokis Small Office Solution platforms, Nokia VPN products and Nokia Message Protector platform do not initiate or terminate SIP based sessions. The mentioned Nokia products are not susceptible to this vulnerability

Nortel Networks

Nortel Networks is cooperating to the fullest extent with the CERT Coordination Center. All Nortel Networks products that use Session Initiation Protocol SIP) have been tested and all generally available products, with the following exceptions, have passed the test suite:

Succession Communication Server 2000 and Succession Communication Server 2000 - Compact are impacted by the test suite only in configurations where SIP-T has been provisioned within the Communication Server; a software patch is expected to be available by the end of February.

For further information about Nortel Networks products please contact Nortel Networks Global Network Support.

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

Contacts for other regions available at the Global Contact< http://www.nortelnetworks.com/help/contact/global/> web page.

Novell

Novell has no products implementing SIP.

Pingtel Corporation

Pingtel has verified that the current versions of software for the Pingtel xpressa desk phone and instant xpressa softphone products, Release 2.1.6, are not vulnerable to any of the tests developed by the University of Oulu and described in CERT Vulnerability Note VU#528719.

Pingtel strongly encourages its customers to use Version 2.1.6. Existing customers may upgrade to this software, free of charge. This software is available at http://www.pingtel.com/s_upgrades.jsp. While the process of updating software for xpressa and instant xpressa can take a phone out of service for two minutes, Pingtel recommends that customers make the effort to stay current, if they aren't already, by upgrading to Version 2.1.6 now. Earlier software revisions are vulnerable, making the use of any release prior to 2.1.6 inadvisable.

Customers that have any questions or concerns are welcome to contact the Pingtel Technical Assistance Center at any time by calling 781-938-5306, emailing support@pingtel.com, or going online at http://support.pingtel.com. Emergency cases are always handled 24 x 7 x 365.

Secure Computing Corporation

Neither Sidewinder nor Gauntlet implements SIP, so we do not need to be on the vendor list for this vulnerability.

SecureWorx

We hereby attest that SecureWorx Basilisk Gateway Security product suite (Firmware version 3.4.2 or later) is NOT VULNERABLE to the Session Initiation Protocol (SIP) Vulnerability VU#528719 as described in the OUSPG announcement (OUSPG#0106) received on Fri, 8 Nov 2002 10:17:11 -0500.

Stonesoft

Stonesoft's StoneGate high availability firewall and VPN product does not contain any code that handles SIP protocol. No versions of StoneGate are vulnerable.

Symantec

Symantec Corporation products are not vulnerable to this issue. Symantec does not implement the Session Initiation Protocol (SIP) in any of our products.

Xerox

Xerox is aware of this vulnerability and is currently assessing all products. This statement will be updated as new information becomes available.

Appendix B References

1. http://www.ee.oulu.fi/research/ouspg/protos/
2. http://www.kb.cert.org/vuls/id/528719
3. http://www.cert.org/tech_tips/denial_of_service.html
4. http://www.ietf.org/html.charters/sip-charter.html
5. RFC3261 - SIP: Session Initiation Protocol
6. RFC2327 - SDP: Session Description Protocol
7. RFC2279 - UTF-8, a transformation format of ISO 10646
8. Session Initiation Protocol Basic Call Flow Examples
9. Session Initiation Protocol Torture Test Messages, Draft

The CERT Coordination Center thanks the Oulu University Secure Programming Group for reporting these vulnerabilities to us, for providing detailed technical analysis, and for assisting us in preparing this advisory. We would also like to acknowledge the "RedSkins" project of "MediaTeam Oulu" for their support of this research.

Feedback on this document can be directed to the authors, Jason A. Rafail and Ian A. Finlay.

Revision History

```
Feb 21, 2003: Initial release

Feb 21, 2003: Added Cisco vendor statement

Feb 21, 2003: Corrected IBM vendor statement

Feb 21, 2003: Added Juniper Networks vendor statement

Feb 24, 2003: Added IBM zSeries vendor statement

Feb 25, 2003: Added Columbia SIP User Agent (sipc) vendor statement

Feb 25, 2003: Revised Columbia SIP User Agent (sipc) vendor statement

Feb 25, 2003: Added Hotsip AB vendor statement

Feb 25, 2003: Added Avaya vendor statement

Feb 27, 2003: Added Dynamicsoft Inc. vendor statement

Mar 06, 2003: Added Check Point vendor statement

Mar 06, 2003: Added Alcatel vendor statement

Mar 07, 2003: Added Ingate Systems vendor statement

Mar 07, 2003: Added Pingtel Corporate vendor statement

Mar 12, 2003: Updated HotSIP AB vendor statement
Mar 13, 2003: Added Cirpack vendor statement

Mar 24, 2003: Added Intoto vendor statement

Mar 24, 2003: Updated Pingtel Corporate vendor statement

Mar 25, 2003: Added Foundry Networks, Inc. vendor statement

Apr 01, 2003: Added Indigo Software vendor statement

Apr 14, 2003: Updated NEC vendor statement

Apr 14, 2003: Added Hughes Software Systems vendor statement

May 09, 2003: Added Mediatrix Telecom, Inc. vendor statement

May 21, 2003: Updated NEC vendor statement
```

7 CA-2003-07: Remote Buffer Overflow in Sendmail

Original release date: March 3, 2003
Last revised: June 09, 2003
Source: CERT/CC

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

Systems Affected

- Sendmail Pro (all versions)
- Sendmail Switch 2.1 prior to 2.1.5
- Sendmail Switch 2.2 prior to 2.2.5
- Sendmail Switch 3.0 prior to 3.0.3
- Sendmail for NT 2.X prior to 2.6.2
- Sendmail for NT 3.0 prior to 3.0.3
- Systems running open-source sendmail versions prior to 8.12.8, including UNIX and Linux systems

Overview

There is a vulnerability in sendmail that may allow remote attackers to gain the privileges of the sendmail daemon, typically root.

I. Description

Researchers at Internet Security Systems (ISS) have discovered a remotely exploitable vulnerability in sendmail. This vulnerability could allow an intruder to gain control of a vulnerable sendmail server.

Most organizations have a variety of mail transfer agents (MTAs) at various locations within their network, with at least one exposed to the Internet. Since sendmail is the most popular MTA, most medium-sized to large organizations are likely to have at least one vulnerable sendmail server. In addition, many UNIX and Linux workstations provide a sendmail implementation that is enabled and running by default.

This vulnerability is message-oriented as opposed to connection-oriented. That means that the vulnerability is triggered by the contents of a specially-crafted email message rather than by lower-level network traffic. This is important because an MTA that does not contain the vulnerability will pass the malicious message along to other MTAs that may be protected at the network level. In other words, vulnerable sendmail servers on the interior of a network are still at risk, even if the site's border MTA uses software other than sendmail. Also, messages capable of exploiting this vulnerability may pass undetected through many common packet filters or firewalls.

Sendmail has indicated to the CERT/CC that this vulnerability has been successfully exploited in a laboratory environment. We do not believe that this exploit is available to the public. However, this vulnerability is likely to draw significant attention from the intruder community, so the probability of a public exploit is high.

A successful attack against an unpatched sendmail system will not leave any messages in the system log. However, on a patched system, an attempt to exploit this vulnerability will leave the following log message:

Dropped invalid comments from header address

Although this does not represent conclusive evidence of an attack, it may be useful as an indicator.

A patched sendmail server will drop invalid headers, thus preventing downstream servers from receiving them.

The CERT/CC is tracking this issue as VU#398025. This reference number corresponds to CVE candidate CAN-2002-1337.

For more information, please see

http://www.sendmail.org

http://www.sendmail.org/8.12.8.html

http://www.sendmail.com/security/

http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950

http://www.kb.cert.org/vuls/id/398025

II. Impact

Successful exploitation of this vulnerability may allow an attacker to gain the privileges of the sendmail daemon, typically root. Even vulnerable sendmail servers on the interior of a given network may be at risk since the vulnerability is triggered from the contents of a malicious email message.

III. Solution

Apply a patch from Sendmail

Sendmail has produced patches for versions 8.9, 8.10, 8.11, and 8.12. However, the vulnerability also exists in earlier versions of the code; therefore, site administrators using an earlier version are encouraged to upgrade to 8.12.8. These patches are located at

ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.security.cr.patch ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.11.6.security.cr.patch

ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.9.3.security.cr.patch

Apply a patch from your vendor

Many vendors include vulnerable sendmail servers as part of their software distributions. We have notified vendors of this vulnerability and recorded their responses in the systems affected section of VU#398025. Several vendors have provided a statement for direct inclusion in this advisory; these statements are available in Appendix A.

Enable the RunAsUser option

There is no known workaround for this vulnerability. Until a patch can be applied, you may wish to set the RunAsUser option to reduce the impact of this vulnerability. As a good general practice, the CERT/CC recommends limiting the privileges of an application or service whenever possible.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Security Update 2003-03-03 is available to fix this issue. Packages are available for Mac OS X 10.1.5 and Mac OS X 10.2.4. It should be noted that sendmail is not enabled by default on Mac OS X, so only those systems which have explicitly enabled it are susceptible to the vulnerability. All customers of Mac OS X, however, are encouraged to apply this update to their systems.

Avaya, Inc.

Avaya is aware of the vulnerability and is investigating impact. As new information is available this statement will be updated.

BSD/OS

Wind River Systems has created patches for this problem which are available from the normal locations for each release. The relevant patches are M500-006 for BSD/OS version 5.0 or the Wind River Platform for Server Appliances 1.0, M431-002 for BSD/OS 4.3.1, or M420-032 for BSD/OS 4.2 systems.

Cisco Systems

Cisco is investigating this issue. If we determine any of our products are vulnerable that information will be available at: http://www.cisco.com/go/psirt

Cray Inc.

The code supplied by Cray, Inc. in Unicos, Unicos/mk, and Unicos/mp may be vulnerable. Cray has opened SPRs 724749 and 724750 to investigate.

Cray, Inc. is not vulnerable for the MTA systems.

Debian

Updated packages for sendmail and sendmail-wide will be available at http://www.debian.org/security/2003/dsa-257

Hewlett-Packard Company

SOURCE:

Hewlett-Packard Company

HP Services

Software Security Response Team

x-ref: SSRT3469

HP released security bulletins for this issue on 03 March 2003

and recently updated 11 March 2003 for Internet Express and

AVFW98.

View at www.hp.com and in the search window type SSRT3469

For HP-UX use your normal ITRC access and select Security

Bulletin HPSBUX0302-246

This problem affects supported versions of HP-UX,

HP Tru64 UNIX/TruCluster Server,

HP AlphaServer SC (Sierra Cluster) V2.5,

HP Internet Express,

HP AltaVista Firewall (AVFW98 / Raptor EC).

NOTE: This problem does not impact

HP NonStop Servers nor HP OpenVMS.

Hitachi, Ltd.

Hitachi's GR2000 gigabit router series

- is NOT vulnerable, because it does not support sendmail.

Hitachi's HI-UX/WE2

- is NOT vulnerable.

If you need technical information, please contact Hitachi's support.

IBM Corporation

The AIX operating system is vulnerable to the sendmail issues discussed in releases 4.3.3, 5.1.0 and 5.2.0.

IBM provides the following official fixes:

APAR number for AIX 4.3.3: IY40500

APAR number for AIX 5.1.0: IY40501

APAR number for AIX 5.2.0: IY40502

Please contact your local IBM AIX support center for any assistance.

Juniper Networks

Sendmail does not ship with any Juniper Networks product, so there is no vulnerability to this issue.

Lotus

IBM has determined that Lotus products, including Notes and Domino, are not vulnerable to the sendmail issues reported by ISS.

MandrakeSoft

MandrakeSoft has issued updated sendmail packages that are not vulnerable to this problem by using the patches provided by the sendmail development team. Users can use urpmi or the Software Manager to upgrade packages. The web advisory is available: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:028

Nortel Networks

The following Nortel Networks Wireless products are potentially affected by the vulnerabilities identified in CERT Advisory CA-2003-07:

> SS7 IP Gateway. Nortel Networks recommends disabling Sendmail as it is not used.
>
> Wireless Preside OAM&P Main Server. Sendmail should not be disabled on these products.

The following Nortel Networks Enterprise Voice IVR products are potentially affected by the vulnerabilities identified in CERT Advisory CA-2003-07:

> MPS1000
>
> MPS500
>
> VPS
>
> CTX

All the above products deploy Sendmail; it should not be disabled on these products.

For all of the above products Nortel Networks recommends applying the latest Sun Microsystems patches in accordance with that vendor's recommendations. To avoid applying patches twice, please ensure that the Sun Microsystems patch applied also addresses the vulnerability identified in CERT Advisory CA-2003-12.

The following Nortel Networks Succession products are potentially affected by the vulnerability identified in CERT Advisory CA-2003-07:

> SSPFS-based CS2000 Management Tools
>
> GWC Element Manager and QoS Collector Application (QCA)
>
> SAM21 Element Manager
>
> Audio Provisioning Server (APS) and APS client GUI
>
> UAS Element Manager
>
> Succession Media Gateway 9000 Element Manager (Mid-Tier and Server)
>
> Network Patch Manager (NPM)
>
> Nodes Configuration, Trunk Configuration, Carrier Endpoint Configuration, Lines Configuration (Servord+), Trunk Maintenance Manager, Lines Maintenance Manager, Line Test Manager, V5.2 Configuration and Maintenance, PM Poller, EMS Proxy Services, and Common Application Launch Point

A product bulletin will be issued shortly.

Sendmail has been disabled in SN06 and therefore SN06 is not vulnerable. A patch for SN05 is currently under development that will disable Sendmail in SN05 so that it will not be affected by the vulnerability identified in CERT Advisory CA-2003-07. The availability date for the SN05 patch is still to be determined.

For more information please contact Nortel at:

> 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/

Openwall GNU/*/Linux

Openwall GNU/*/Linux is not vulnerable. We use Postfix as the MTA, not sendmail.

Postfix

Postfix 2.0.6 duplicates the Sendmail 8.12.8 fix to in order to help protect downstream Sendmail systems against exploitation of this vulnerability. Patches are also available for several older Postfix releases. For download information, please see http://www.postfix.org/.

Red Hat Inc.

Updated sendmail packages that are not vulnerable to this issue are available for Red Hat Linux, Red Hat Advanced Server, and Red Hat Advanced Workstation. Red Hat Network users can update their systems using the 'up2date' tool.

Red Hat Linux:

http://rhn.redhat.com/errata/RHSA-2003-073.html

Red Hat Linux Advanced Server, Advanced Workstation:

http://rhn.redhat.com/errata/RHSA-2003-074.html

Sequent Computer Systems (IBM)

For information please contact IBM Service at 1-800-IBM-SERV.

SGI

SGI acknowledges VU#398025 reported by CERT and has released an advisory to address the vulnerability on IRIX.

Refer to SGI Security Advisory 20030301-01-P available from ftp://patches.sgi.com/support/free/security/advisories/20030301-01-P or http://www.sgi.com/support/security/.

The Sendmail Consortium

The Sendmail Consortium suggests that sites upgrade to 8.12.8 if possible. Alternatively, patches are available for 8.9, 8.10, 8.11, and 8.12 on http://www.sendmail.org/

Sendmail, Inc.

All commercial releases including Sendmail Switch, Sendmail Advanced Message Server (which includes the Sendmail Switch MTA), Sendmail for NT, and Sendmail Pro are affected by this issue. Patch information is available at http://www.sendmail.com/security.

Sun Microsystems

Solaris 2.6, 7, 8 and 9 are vulnerable to VU#398025.

Sun will be publishing a Sun Alert for the issue at the following location shortly:

http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/51181

The patches listed in the Sun Alert will be available from:

http://sunsolve.sun.com/securitypatch

Syntegra

None of Syntegra's mail products, including IntraStore, eMail Sentinel and Mail*Hub are vulnerable to this defect.

Xerox Corporation

A response to this advisory is available from our web site: http://www.xerox.com/security.

Our thanks to Internet Security Systems, Inc. for discovering this problem, and to Eric Allman, Claus Assmann, and Greg Shapiro of Sendmail for notifying us of this problem. We thank both groups for their assistance in coordinating the response to this problem.

Authors: Jeffrey P. Lanza and Shawn V. Hernan

Revision History

```
Mar 03, 2003: Initial release

Mar 03, 2003: Added statement for Sun Microsystems

Mar 03, 2003: Fixed typo in mailto: URL
```

Mar 04, 2003: Added statements for Juniper Networks, MandrakeSoft, and Hitachi

Mar 04, 2003: Added statement for Debian

Mar 04, 2003: Added statement for Lotus

Mar 10, 2003: Added statement for Postfix

Mar 12, 2003: Updated statement for Hewlett-Packard

Mar 13, 2003: Updated statement for IBM

Mar 27, 2003: Updated statement for Hitachi

Apr 22, 2003: Added statement for Nortel Networks; statement submitted on 8-Apr-2003

Jun 09, 2003: Added statements for Sequent, Syntegra, and Xerox

8 CA-2003-08: Increased Activity Targeting Windows Shares

Original release date: March 11, 2003
Source: CERT/CC

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

Systems Affected

- Microsoft Windows 2000
- Microsoft Windows XP

Overview

In recent weeks, the CERT/CC has observed an increase in the number of reports of systems running Windows 2000 and XP compromised due to poorly protected file shares.

I. Description

Over the past few weeks, the CERT/CC has received an increasing number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak *Administrator* passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor, which are described in more detail below.

Background

Microsoft Windows uses the SMB protocol to share files and printer resources with other computers. In older versions of Windows (e.g., 95, 98, Me, and NT), SMB shares ran on NetBIOS over TCP/IP (NBT) on ports 137/tcp and udp, 138/udp, and 139/tcp. However, in later versions of Windows (e.g., 2000 and XP), it is possible to run SMB directly over TCP/IP on port 445/tcp.

Windows file shares with poorly chosen or Null passwords have been a recurring security risk for both corporate networks and home users for some time:

- IN-2002-06: W32/Lioten Malicious Code
- CA-2001-20: Continuing Threats to Home Users
- IN-2000-02: Exploitation of Unprotected Windows Networking Shares
- IN-2000-03: 911 Worm

It has often been the case that these poorly configured shares were exposed to the Internet. Intruders have been able to leverage poorly protected Windows shares by exploiting weak or Null passwords to access user-created and default administrative shares. This problem is exacerbated by another relevant trend: intruders specifically targeting Internet address ranges known to contain a high density of weakly protected systems. As described in CA-2001-20, the intruders' efforts commonly focus on addresses known to be used by home broadband connections.

Recent developments

The CERT/CC has recently received a number of reports of exploitation of Null or weak *Administrator* passwords on systems running Windows 2000 or Windows XP. Thousands of systems have been compromised in this manner.

Although the tools involved in these reports vary, they exhibit a number of common traits, including

- scanning for systems listening on 445/tcp (frequently within the same /16 network as the infected host)
- exploiting Null or weak passwords to gain access to the *Administrator* account
- opening backdoors for remote access
- connecting back to Internet Relay Chat (IRC) servers to await additional commands from attackers
- installing or supporting tools for use in distributed denial-of-service (DDoS) attacks

Some of the tools reported have self-propagating (i.e., worm) capabilities, while others are propagated via social engineering techniques similar to those described in IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging.

The network scanning associated with this activity is widespread but appears to be especially concentrated in address ranges commonly associated with home broadband users. Using these techniques, many attackers have built sizable networks of DDoS agents, each comprised of thousands of compromised systems.

W32/Deloder

The self-propagating W32/Deloder malicious code is an example of the intruder activity described above. It begins by scanning the /16 (i.e., addresses with the same first two high-order octets) of the infected host for systems listening on 445/tcp. When a connection is established, W32/Deloder attempts to compromise the *Administrator* account by using a list of pre-loaded passwords. Variants may include different or additional passwords, but reports to the CERT/CC indicate that the following have appeared thus far:

```
[NULL] 0 000000 00000000 007 1 110 111 111111 11111111 12
121212 123 123123 1234 12345 123456 1234567 12345678 123456789
1234qwer 123abc 123asd 123qwe 2002 2003 2600 54321 654321
88888888 Admin Internet Login Password a aaa abc abc123 abcd
admin admin123 administrator alpha asdf computer database ena-
ble foobar god godblessyou home ihavenopass login love mypass
```

```
mypass123 mypc mypc123 oracle owner pass passwd password pat
patrick pc pw pw123 pwd qwer root secret server sex super
sybase temp temp123 test test123 win xp xxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx yxcv zxcv
```

On successful compromise of the *Administrator* account, W32/Deloder copies itself to the victim, placing multiple copies in various locations on the system. Additionally, it adds a registry key that will cause the automatic execution of `dvldr32.exe` (one of the aforementioned copies). The victim will begin scanning for other systems to infect after it is restarted.

W32/Deloder opens up backdoors on the victim system to allow attackers further access. It does this in two ways:

1. attempting to connect to one of a number of pre-configured IRC servers
2. installing a copy of VNC (Virtual Network Computing), an open-source remote display tool from AT&T, listening on 5800/tcp or 5900/tcp

Note: VNC in and of itself is not a malicious tool, and has many other legitimate uses.

During the course of infection by W32/Deloder, a number of files may be created on the system. Reports indicate that files matching the following descriptions have been found on compromised systems:

Filename	**File Size (bytes)**	**Description**
`dvldr32.exe`	745,984	The self-propagating malicious code
`inst.exe`	684,562	This file installs the backdoor applications onto the victim host
`psexec.exe`	36,352	A copy of the Remote Process Launch application (not inherently malicious, but it is what allows the worm to replicate)
`explorer.exe`	212,992	A renamed copy of the VNC application
`omnithread_rt.dll`	57,344	VNC dependency file
`VNCHooks.dll`	32,768	VNC dependency file

`rundll32.exe`	29,336	The IRC-Pitchfork bot application
`cygwin1.dll`	944,968	IRC-Pitschfork dependency file

GT-bot and sdbot

Intruders frequently use IRC "bots" (automated software that accepts commands via IRC channels) to remotely control compromised systems. GT-bot and sdbot are two examples of intruder-developed IRC bots. Both support automated scanning and exploitation of inadequately protected Windows shares. These tools also offer intruders a variety of DDoS capabilities, including the ability to generate ICMP, UDP, or TCP traffic.

Tools like these are undergoing constant development in the intruder community and are frequently included as part of other tools. As a result, the names, sizes, and other characteristics of the files that might contain these tools vary widely. Furthermore, once installed, the tools are designed to hide themselves fairly well, so detection may be difficult.

The CERT/CC has received reports of sdbot networks as large as 7,000 systems, and GT-bot networks in excess of 140,000 systems.

W32/Slackor

The W32/Slackor worm is another example of a tool that targets file shares. On a compromised machine, the worm begins by scanning the /16 of the infected host for other systems listening on 445/tcp. When a system is discovered, W32/Slackor connects to the $IPC share using a set of pre-programmed usernames and passwords, copies itself to the `C:\sp` directory, and runs its payload. The payload consists of the following files:

Filename	**Description**
`slackeworm.exe`	The self-propagating malicious code
`abc.bat`	List of usernames/passwords
`psexec.exe`	A copy of the Remote Process Launch application (from sysinternals.com, used for replicating the worm)
`main.exe`	The bot application

W32/Slackor also contains an IRC bot. When this bot joins its IRC network, a remote intruder controlling the IRC channel can issue arbitrary commands on the compromised computer, including launching denial-of-service attacks.

Network footprint

Widespread scanning for 445/tcp indicates activity of this type. Compromised hosts may also have unauthorized connections to IRC servers (typically on 6667/tcp, although ports may vary). Additionally, the VNC package installed by W32/Deloder will typically listen on 5800/tcp or 5900/tcp. If a compromised system is used in a DDoS attack on another site, large volumes of IP traffic (ICMP, UDP, or TCP) may be detected emanating from the compromised system.

II. Impact

The presence of any of these tools on a system indicates that the *Administrator* password has likely been compromised, and the entire system is therefore suspect. With this level of access, intruders may

- exercise remote control
- expose confidential data
- install other malicious software
- change files
- delete files
- launch attacks against other sites

The scanning activities of these tools may generate high volumes of 445/tcp traffic. As a result, some Internet-connected hosts or networks with compromised hosts may experience performance issues (including denial-of-service conditions).

Sites targeted by the DDoS agents installed by this activity may experience unusually heavy traffic volumes or high packet rates, resulting in degradation of services or loss of connectivity altogether.

III. Solution

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

Disable or secure file shares

Best practice dictates a policy of least privilege; if a given computer is not intended to be a server (i.e., share files with others), "File and Printer Sharing for Microsoft Networks" should be disabled.

For computers that export shares, ensure that user authentication is required and that each account has a well-chosen password. Furthermore, consider using a firewall to control which computer can access these shares.

By default, Windows NT, 2000, and XP create certain hidden and administrative shares. See the HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers for further guidelines on managing these shares.

Use strong passwords

The various tools described above exploit the use of weak or Null passwords in order to propagate, so using strong passwords can help keep them from infecting your systems.

Microsoft has posted a "Create Strong Passwords" checklist.

Run and maintain an anti-virus product

The malicious code being distributed in these attacks is under continuous development by intruders, but most anti-virus software vendors release frequently updated information, tools, or virus databases to help detect and recover from the malicious code involved in this activity. Therefore, it is important that users keep their anti-virus software up to date. The CERT/CC maintains a partial list of anti-virus vendors.

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

Do not run programs of unknown origin

Never download, install, or run a program unless you know it to be authored by a person or company that you trust. Users of IRC, Instant Messaging (IM), and file-sharing services should be particularly wary of following links or running software sent to them by other users, as this is a commonly used method among intruders attempting to build networks of DDoS agents.

Deploy a firewall

The CERT/CC also recommends using a firewall product, such as a network appliance or a personal firewall software package. In some situations, these products may be able to alert users to the fact that their machine has been compromised. Furthermore, they have the ability to block intruders from accessing backdoors over the network. However, no firewall can detect or stop all attacks, so it is important to continue to follow safe computing practices.

Ingress/egress filtering

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. In the network usage policy of many sites, external hosts are only permitted to initiate inbound traffic to machines that provide public services on specific ports. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services.

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for internal systems to access SMB shares across the Internet.

In the case of the intruder activity described above, blocking connections to port 445/tcp from entering or leaving your network reduces the risk of external infected systems attacking hosts inside your network or vice-versa.

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

IV. References

1. Trends in Denial of Service Attack Technology: http://www.cert.org/archive/pdf/DoS_trends.pdf
2. Managing the Threat of Denial-of-Service Attacks: http://www.cert.org/archive/pdf/Managing_DoS.pdf
3. IN-2002-06: W32/Lioten Malicious Code: http://www.cert.org/incident_notes/IN-2002-06.html
4. CA-2001-20: Continuing Threats to Home Users: http://www.cert.org/advisories/CA-2001-20.html
5. IN-2000-02: Exploitation of Unprotected Windows Networking Shares: http://www.cert.org/incident_notes/IN-2000-02.html
6. IN-2000-03: 911 Worm: http://www.cert.org/incident_notes/IN-2000-03.html
7. IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging: http://www.cert.org/incident_notes/IN-2002-03.html
8. VNC (Virtual Network Computing): http://www.uk.research.att.com/vnc/
9. Home Network Security: http://www.cert.org/tech_tips/home_networks.html
10. Home Computer Security: http://www.cert.org/homeusers/HomeComputerSecurity/
11. HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q314984&sd=tech
12. Checklist: Create Strong Passwords: http://www.microsoft.com/security/articles/password.asp
13. Anti-virus vendors: http://www.cert.org/other_sources/viruses.html#VI
14. Steps for Recovering from a UNIX or NT System Compromise: http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#36888]".

Feedback can be directed to the authors: Allen Householder and Roman Danyliw

Revision History

```
March 11, 2003: Initial release
```

9 CA-2003-09: Buffer Overflow in Microsoft IIS 5.0

Original issue date: March 17, 2003
Last revised: Fri Apr 25 14:10:29 EDT 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Windows 2000
- Systems running Windows NT 4.0

Overview

A buffer overflow vulnerability exists in the Win32 API libraries shipped with all versions of Microsoft Windows 2000 and Microsoft Windows NT 4.0. This vulnerability, which is being actively exploited on WebDAV-enabled IIS 5.0 servers, will allow a remote attacker to execute arbitrary code on unpatched systems. Sites running Microsoft Windows 2000 and Microsoft Windows NT 4.0 should apply a patch or disable WebDAV services as soon as possible.

I. Description

Microsoft Windows 2000 (and possibly prior versions of Windows) contains a dynamic link library (DLL) named ntdll.dll. This DLL is a core operating system component used to interact with the Windows kernel. A buffer overflow vulnerability exists in ntdll.dll, which is utilized by many different components in the Windows operating system.

The WebDAV (RFC2518) component of Microsoft IIS 5.0 is an example of one Windows component that uses ntdll.dll. The IIS WebDAV component utilizes ntdll.dll when processing incoming WebDAV requests. By sending a specially crafted WebDAV request to an IIS 5.0 server, an attacker may be able to execute arbitrary code in the Local System security context, essentially giving the attacker complete control of the system.

Because the vulnerable Win32 API component is utilized by many other applications, it is possible other exploit vectors exist. However, we have only been told of systems compromised running IIS 5.0 with WebDAV enabled. Sites using Windows 2000 but not running IIS 5.0 with WebDAV need to carefully weigh the trade-offs before applying patches to systems where the core vulnerability exists but may not be exploitable.

Microsoft has issued the following bulletin regarding this vulnerability:

> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-007.asp

This vulnerability has been assigned the identifier CAN-2003-0109 by the Common Vulnerabilities and Exposures (CVE) group:

> http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109

II. Impact

Any attacker who can reach a vulnerable web server can gain complete control of the system and execute arbitrary code in the Local System security context. Note that this may be significantly more serious than a simple "web defacement."

III. Solution

Apply a patch from your vendor

A patch is available from Microsoft at

> http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en

Note that, according to MS03-007, "Microsoft was made aware that some customers who had received a hotfix from Product Support Services experienced stop errors on boot after applying the patch released for this bulletin." For more information, see the "Frequently asked questions" section of MS03-007.

Disable vulnerable service

Until a patch can be applied, you may wish to disable IIS:

> http://support.microsoft.com/default.aspx?scid=kb;en-us;321141

If you cannot disable IIS, consider using the IIS lockdown tool to disable WebDAV (removing WebDAV can be specified when running the IIS lockdown tool). Alternatively, you can disable WebDAV by following the instructions located in Microsoft's Knowledgebase Article 241520, "How to Disable WebDAV for IIS 5.0":

> http://support.microsoft.com/default.aspx?scid=kb;en-us;241520

Restrict buffer size

If you cannot use the IIS lockdown tool, consider restricting the size of the buffer IIS utilizes to process requests by using Microsoft's URL Buffer Size Registry Tool. This tool can be run against a local or remote Windows 2000 system running Windows 2000 Service Pack 2 or Service Pack 3. The tool, instructions on how to use it, and instructions on how to manually make changes to the registry are available here:

URL Buffer Size Registry Tool - http://go.microsoft.com/fwlink/?LinkId=14875
Microsoft Knowledge Base Article 816930 - http://support.microsoft.com/default.aspx?scid=kb;en-us;816930
Microsoft Knowledge Base Article 260694 - http://support.microsoft.com/default.aspx?scid=kb;en-us;260694

You may also wish to use URLScan, which will block web requests that attempt to exploit this vulnerability. Information about URLScan is available at

http://support.microsoft.com/default.aspx?scid=kb;[LN];326444

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft Corporation

Please see Microsoft Security Bulletin MS03-007.

The CERT/CC thanks Microsoft for their feedback during the preparation of this document. We also thank the Department of Education Network Engineering group for their contributions.

Authors: Ian A. Finlay & Jeffrey S. Havrilla

Revision History

March 17, 2003: Initial release

March 17, 2003: Changed overview section to reflect IIS 5.0 enabled by default on Windows 2000 server products

March 19, 2003: Changed title from "Buffer Overflow in Microsoft IIS 5.0" to "Buffer Overflow in Core Microsoft Windows DLL"

March 19, 2003: Changed overview and description to reflect fact that vulnerability is in core system DLL

March 19, 2003: Revised section on disabling IIS

April 25, 2003: Revised Systems affected to include Microsoft Windows NT 4.0

10 CA-2003-10: Integer overflow in Sun RPC XDR library routines

Original release date: March 19, 2003
Last revised: April 9, 2003
Source: CERT/CC

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

Systems Affected

Applications using vulnerable implementations of SunRPC-derived XDR libraries, which include

- Sun Microsystems network services library (libnsl)
- BSD-derived libraries with XDR/RPC routines (libc)
- GNU C library with sunrpc (glibc)

Overview

There is an integer overflow in the *xdrmem_getbytes()* function distributed as part of the Sun Microsystems XDR library. This overflow can cause remotely exploitable buffer overflows in multiple applications, leading to the execution of arbitrary code. Although the library was originally distributed by Sun Microsystems, multiple vendors have included the vulnerable code in their own implementations.

I. Description

XDR (external data representation) libraries are used to provide platform-independent methods for sending data from one system process to another, typically over a network connection. Such routines are commonly used in remote procedure call (RPC) implementations to provide transparency to application programmers who need to use common interfaces to interact with many different types of systems. The *xdrmem_getbytes()* function in the XDR library provided by Sun Microsystems contains an integer overflow that can lead to improperly sized dynamic memory allocation. Depending on how and where the vulnerable *xdrmem_getbytes()* function is used, subsequent problems like buffer overflows may result.

Researchers at eEye Digital Security discovered this vulnerability and have also published an advisory. This issue is currently being tracked as VU#516825 by the CERT/CC and as CAN-2003-0028 in the Common Vulnerabilities and Exposures (CVE) dictionary. Note that this vulnerability is similar to, but distinct from, VU#192995.

II. Impact

Because SunRPC-derived XDR libraries are used by a variety of vendors in a variety of applications, this defect may lead to a number of security problems. Exploiting this vulnerability will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information.

Specific impacts reported include the ability to crash the rpcbind service and possibly execute arbitrary code with root privileges. In addition, intruders may be able to crash the MIT KRB5 kadmind or cause it to leak sensitive information, such as secret keys.

III. Solution

Apply a patch from your vendor

Apply the appropriate patch or upgrade as specified by your vendor. See Appendix A below and the Systems Affected section of VU#516825 for further information.

Note that XDR libraries can be used by multiple applications on most systems. It may be necessary to upgrade or apply multiple patches and then recompile statically linked applications.

Applications that are statically linked must be recompiled using patched libraries. Applications that are dynamically linked do not need to be recompiled; however, running services need to be restarted in order to use the patched libraries.

System administrators should consider the following process when addressing this issue:

1. Patch or obtain updated XDR/RPC libraries.
2. Restart any dynamically linked services that make use of the XDR/RPC libraries.
3. Recompile any statically linked applications using the patched or updated XDR/RPC libraries.

Disable access to vulnerable services or applications

Until patches are available and can be applied, you may wish to disable access to services or applications compiled with the vulnerable *xdrmem_getbytes()* function.

As a best practice, the CERT/CC recommends disabling all services that are not explicitly required.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server do not contain the vulnerabilities described in this report.

Cray, Inc.

Cray Inc. may be vulnerable and has opened spr's 724153 and 724154 to investigate.

Fujitsu

We are currently investigating how the vulnerability reported under VU#516825 affects the Fujitsu UXP/V O.S. We will update this statement as soon as new information becomes available.

GNU glibc

Version 2.3.1 of the GNU C Library is vulnerable. Earlier versions are also vulnerable. The following patches have been installed into the CVS sources, and should appear in the next version of the GNU C Library. These patches are also available from the following URLs:

http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/rpc/xdr.h.diff?r1=1.26&r2=1.27&cvsroot=glibc
http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_mem.c.diff?r1=1.13&r2=1.15&cvsroot=glibc
http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_rec.c.diff?r1=1.26&r2=1.27&cvsroot=glibc
http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_sizeof.c.diff?r1=1.5&r2=1.6&cvsroot=glibc
http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_stdio.c.diff?r1=1.15&r2=1.16&cvsroot=glibc

```
2002-12-16 Roland McGrath

* sunrpc/xdr_mem.c (xdrmem_inline): Fix argument type.

* sunrpc/xdr_rec.c (xdrrec_inline): Likewise.

* sunrpc/xdr_stdio.c (xdrstdio_inline): Likewise.

2002-12-13 Paul Eggert

* sunrpc/rpc/xdr.h (struct XDR.xdr_ops.x_inline): 2nd arg

is now u_int, not int.

(struct XDR.x_handy): Now u_int, not int.

* sunrpc/xdr_mem.c: Include .

(xdrmem_getlong, xdrmem_putlong, xdrmem_getbytes, xdrmem_putbytes,

xdrmem_inline, xdrmem_getint32, xdrmem_putint32):

x_handy is now unsigned, not signed.
```

```
Do not decrement x_handy if no change is made.

(xdrmem_setpos): Check for int overflow.

* sunrpc/xdr_sizeof.c (x_inline): 2nd arg is now unsigned.

(xdr_sizeof): Remove cast that is now unnecessary, now that

x_handy is unsigned.
```

[text of diffs available in the links included above --CERT/CC]

Hewlett-Packard Company

RE: HP Case ID SSRT2439

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products.

As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

Hitachi

Hitachi's GR2000 gigabit router series - is NOT vulnerable.

Hitachi's HI-UX/WE2 - is NOT vulnerable, because it does not support RPC/XDR Library.

IBM Corporation

The AIX operating system is vulnerable to the issues discussed in CERT vulnerability note VU#516825 in releases 4.3.3, 5.1.0 and 5.2.0.

IBM provides the following official fixes:

APAR number for AIX 4.3.3: IY38524
APAR number for AIX 5.1.0: IY38434
APAR number for AIX 5.2.0: IY39231

Please contact your local IBM AIX support center for any assistance.

Ingrian Networks

Ingrian Networks products are not succeptable to the vulnerabilities in VU#516825.

MIT Kerberos Development Team

It may be possible for a remote attacker to exploit an integer overflow in xdrmem_getbytes() to crash the kadmind server process by a read segmentation fault. For this to succeed, the kadmind process must be able to allocate more than MAX_INT bytes of memory. This is believed to be unlikely, as most installations are not likely to permit that the allocation of that much memory.

It may also be possible for a remote attacker to exploit this integer overflow to obtain sensitive information, such as secret keys, from the kadmind process. This is believed to be extremely unlikely, as there are unlikely to be ways for the information, once improperly copied, of being returned to the attacker. In addition, the above condition of the kadmind being able to allocate huge amounts of memory must be satisfied.

Please see http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-003-xdr.txt

This patch may also be found at:
http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt

The associated detached PGP signature is at:

http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt.asc

NEC Corporation

[Server Products] * EWS/UP 48 Series operating system - is NOT vulnerable.

NetBSD

The length types of the various xdr*_getbytes functions were made consistent somewhere back in 1997 (all u_int), so we're not vulnerable in that area.

[Note: the NetBSD project has released NetBSD Security Advisory 2003-008 in response to this issue --CERT/CC]

Network Appliance

NetApp products are not vulnerable to this issue.

Nokia

This issue has no relationship to the product we ship.

Nortel Networks

The following Nortel Networks Wireless products are potentially affected by the vulnerability identified in VU#516825:

CDMA SDMX
CS2000 SSPFS
GBMD (GSM Billing Mediation Device)
GSM CIPC
SS7IP Gateway
OAM&P Main & Performance Servers

Nortel Networks recommends applying the latest Sun Microsystems patches in accordance with that vendor's recommendations.

Other Nortel Networks products are being investigated to determine if they are potentially affected by the vulnerability identified in VU#516825 and this statement will be updated as more information becomes available.

Openwall GNU/*/Linux

The xdrmem_getbytes() integer overflow discovered by eEye Digital Security was present in the glibc package on Openwall GNU/*/Linux until 2003/03/23 when it was corrected for Owl-current (with a back-port from the glibc CVS) and documented as a security fix in the system-wide change log available at:

http://www.openwall.com/Owl/CHANGES-current.shtml

Please note that Owl does not include any RPC services (but it does include a few RPC clients). It has not been fully researched whether an Owl install with no third-party software added is affected by this vulnerability at all.

SGI

SGI acknowledges receiving CERT VU#516825 and is currently investigating. This is being tracked as SGI Bug# 880925. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported SGI operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on http://www.sgi.com/support/security/

[Note: SGI has subsequently released SGI Security Advisory 20030402-01-P in response to this issue. Users are encouraged to review this advisory and apply the patches it refers to. --CERT/CC]

Sun Microsystems

Solaris 2.6, 7, 8 and 9 are vulnerable to VU#516825.

Sun will be publishing a Sun Alert for the issue at the following location shortly: http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/51884

The Sun Alert will be updated with the patch information as soon as the patches are available.

At that time, the patches listed in the Sun Alert will be available from: http://sunsolve.sun.com/securitypatch

Top Layer Networks

Top Layer Networks products do not contain the vulnerabilities described in this CERT Advisory.

Appendix B References

1. AD20030318.html - http://www.eeye.com/html/Research/Advisories/AD20030318.html
2. VU#192995 - http://www.kb.cert.org/vuls/id/192995
3. VU#516825 - http://www.kb.cert.org/vuls/id/516825
4. RFC1831 - http://www.ietf.org/rfc/rfc1831.txt
5. RFC1832 - http://www.ietf.org/rfc/rfc1832.txt

Thanks to Riley Hassell of eEye Digital Security for discovering and reporting this vulnerability. Thanks also to Sun Microsystems for additional technical details.

Authors: Chad Dougherty and Jeffrey Havrilla

Revision History

```
Mar 19, 2003: Initial release

Mar 20, 2003: Updated vendor statement from Hitachi

Mar 24, 2003: Added vendor statement for Openwall GNU/*/Linux

Apr 01, 2003: Added vendor statement for Top Layer Networks, updated
vendor statement for NetBSD

Apr 09, 2003: Added vendor statement for Nortel Networks, updated
vendor statement for SGI
```

11 CA-2003-11: Multiple Vulnerabilities in Lotus Notes and Domino

Original release date: March 26, 2003
Last revised: Apr 02, 2003
Source: CERT/CC

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

Systems Affected

- Lotus Notes and Domino versions prior to 5.0.12 and 6.0 Gold
- VU#571297 affects 5.0.12, 6.0.1 and prior versions.

Overview

Multiple vulnerabilities have been reported to affect Lotus Notes clients and Domino servers. Multiple reporters, the close timing, and some ambiguity caused confusion about what releases are vulnerable. We are issuing this advisory to help clarify the details of the vulnerabilities, the versions affected, and the patches that resolve these issues.

I. Description

In February 2003, NGS Software released several advisories detailing vulnerabilities affecting Lotus Notes and Domino. The following vulnerabilities reported by NGS Software affect versions of Lotus Domino prior to 5.0.12 and 6.0:

VU#206361 - Lotus iNotes vulnerable to buffer overflow via PresetFields FolderName field
Lotus Technical Documentation: KSPR5HUQ59
NGS Software's Advisory: NISR17022003b

VU#355169 - Lotus Domino Web Server vulnerable to denial of service via incomplete POST request
Lotus Technical Documentation: KSPR5HTQHS
NGS Software's Advisory: NISR17022003d

VU#542873 - Lotus iNotes vulnerable to buffer overflow via PresetFields s_ViewName field
Lotus Technical Documentation: KSPR5HUPEK
NGS Software's Advisory: NISR17022003b

VU#772817 - Lotus Domino Web Server vulnerable to buffer overflow via non-existent "h_SetReturnURL" parameter with an overly long "Host Header" field

Lotus Technical Documentation: KSPR5HTLW6
NGS Software's Advisory: NISR17022003a

The following vulnerability reported by NGS Software affects versions of Lotus Domino up to and including 5.0.12 and 6.0.1:

VU#571297 - Lotus Notes and Domino COM Object Control Handler contains buffer overflow
Lotus Technical Documentation: SWG21104543
NGS Software's Advisory: NISR17022003e

VU#571297 was originally reported as a vulnerability in an iNotes ActiveX control. The vulnerable code is not specific to iNotes or ActiveX. The iNotes ActiveX control was an attack vector for the vulnerability and is not the affected code base. Because this issue is not specific to ActiveX, Lotus Notes clients and Domino Servers running on platforms other than Microsoft Windows may be affected.

In March 2003, Rapid7, Inc. released several advisories. The following vulnerabilities, reported by Rapid7, Inc., affect versions of Lotus Domino prior to 5.0.12:

VU#433489 - Lotus Domino Server susceptible to a pre-authentication buffer overflow during Notes authentication
Lotus Technical Documentation: DBAR5CJJJS
Rapid7, Inc.'s Advisory: R7-0010

VU#411489 - Lotus Domino Web Retriever contains a buffer overflow vulnerability
Lotus Technical Documentation: KSPR5DFJTR
Rapid7, Inc.'s Advisory: R7-0011

Rapid7, Inc. also discovered that Lotus Domino pre-release and beta versions of 6.0 were also affected by the following vulnerability:

VU#583184 - Lotus Domino R5 Server Family contains multiple vulnerabilities in LDAP handling code
Lotus Technical Documentation: DWUU4W6NC8
Rapid7, Inc.'s Advisory: R7-0012

The release version of Lotus Domino 6.0 is not affected. Only pre-release and beta versions of 6.0 are affected. VU#583184 was a regression of the PROTOS LDAP Test-Suite from CA-2001-18 and was originally fixed in 5.0.7a.

II. Impact

The impact of these vulnerabilities range from denial of service to data corruption and the potential to execute arbitrary code. For details about the impact of a specific vulnerability, please see the related vulnerability note.

III. Solution

Upgrade

Most of these vulnerabilities are resolved in versions 5.0.12 and 6.0.1 of Lotus Domino.

Only VU#571297, "Lotus Notes and Domino COM Object Control Handler contains buffer overflow," is not resolved in 5.0.12, or 6.0.1. Critical Fix 1 for 6.0.1 was released on March 18, 2003, to resolve this issue for both the Notes client and Domino server.

Apply a patch

Patches are available for some vulnerabilities. Please view the individual vulnerability notes for specific patch information.

Block access from outside the network perimeter

Lotus Domino servers listen on port 1352/TCP. Notes may also be configured to listen on other ports, such as NETBIOS, SPX, or XPC. Blocking access to these ports from machines outside your trusted network perimeter may help mitigate successful exploitation of these vulnerabilities.

Appendix A References

1. http://www.kb.cert.org/vuls/id/571297
2. http://www.kb.cert.org/vuls/id/206361
3. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=KSPR5HUQ59
4. http://www.nextgenss.com/advisories/lotus-inotesoflow.txt
5. http://www.kb.cert.org/vuls/id/355169
6. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=KSPR5HTQHS
7. http://www.nextgenss.com/advisories/lotus-60dos.txt
8. http://www.kb.cert.org/vuls/id/542873
9. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=KSPR5HUPEK
10. http://www.nextgenss.com/advisories/lotus-inotesoflow.txt
11. http://www.kb.cert.org/vuls/id/772817
12. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=KSPR5HTLW6
13. http://www.nextgenss.com/advisories/lotus-hostlocbo.txt
14. http://www.kb.cert.org/vuls/id/571297
15. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=swg21104543
16. http://www.nextgenss.com/advisories/lotus-inotesclientaxbo.txt
17. http://www.kb.cert.org/vuls/id/433489
18. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=DBAR5CJJJS
19. http://www.rapid7.com/advisories/R7-0010.html
20. http://www.kb.cert.org/vuls/id/411489

21. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=KSPR5DFJTR
22. http://www.rapid7.com/advisories/R7-0011.html
23. http://www.kb.cert.org/vuls/id/583184
24. http://www.ibm.com/Search?v=11&lang=en&cc=us&q=DWUU4W6NC8
25. http://www.rapid7.com/advisories/R7-0012.html
26. http://www.kb.cert.org/vuls/id/583184
27. http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3/
28. http://www.cert.org/advisories/CA-2001-18.html
29. http://www.kb.cert.org/vuls/id/571297
30. http://www-10.lotus.com/ldd/r5fixlist.nsf/80bff5d07b4be477052569ce00710588/8bc951d3ff1e578385256ce10052a78a?OpenDocument

Our thanks to NGS Software and Rapid7, Inc. for discovering and reporting on these vulnerabilities. We also thank the Lotus Security Team for aiding in the resolution and clarification of these issues.

Feedback on this document can be directed to the author, Jason A. Rafail.

Revision History

```
Mar 26, 2003: Initial release

Apr 02, 2003: Added Clarification that VU#583184 does not affect the

release version of Lotus Domino 6.0, only pre-release and beta versions.
```

12 CA-2003-12: Buffer Overflow in Sendmail

Original release date: March 29, 2003
Last revised: May 29, 2003
Source: CERT/CC

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

Systems Affected

- Sendmail Pro (all versions)
- Sendmail Switch 2.1 prior to 2.1.6
- Sendmail Switch 2.2 prior to 2.2.6
- Sendmail Switch 3.0 prior to 3.0.4
- Sendmail for NT 2.X prior to 2.6.3
- Sendmail for NT 3.0 prior to 3.0.4
- Systems running open-source sendmail versions prior to 8.12.9, including UNIX and Linux systems

Overview

There is a vulnerability in sendmail that can be exploited to cause a denial-of-service condition and could allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon, typically root.

I. Description

There is a remotely exploitable vulnerability in sendmail that could allow an attacker to gain control of a vulnerable sendmail server. Due to a variable type conversion problem (`char` to `signed int`), sendmail may not adequately check the length of address tokens. A specially crafted email message could trigger a stack overflow. This vulnerability was discovered by Michal Zalewski.

This vulnerability is different than the one described in CA-2003-07.

Most organizations have a variety of mail transfer agents (MTAs) at various locations within their network, with at least one exposed to the Internet. Since sendmail is the most popular MTA, most medium-sized to large organizations are likely to have at least one vulnerable sendmail server. In addition, many UNIX and Linux workstations provide a sendmail implementation that is enabled and running by default.

This vulnerability is message-oriented as opposed to connection-oriented. That means that the vulnerability is triggered by the contents of a specially-crafted email message rather than by lower-level network traffic. This is important because an MTA that does not contain the vulnerability will pass the malicious message along to other MTAs that may be protected at the network level. In other words, vulnerable sendmail servers on the interior of a network are still at risk, even if the site's border MTA uses software other than sendmail. Also, messages capable of exploiting this vulnerability may pass undetected through many common packet filters or firewalls.

This vulnerability has been successfully exploited to cause a denial-of-service condition in a laboratory environment. It is possible that this vulnerability could be used to execute arbitrary code on some vulnerable systems.

The CERT/CC is tracking this issue as VU#897604. This reference number corresponds to CVE candidate CAN-2003-0161.

For more information, please see

http://www.sendmail.org

http://www.sendmail.org/8.12.9.html

http://www.sendmail.com/security/

For the latest information about this vulnerability, including the most recent vendor information, please see

http://www.kb.cert.org/vuls/id/897604

This vulnerability is distinct from VU#398025.

II. Impact

Successful exploitation of this vulnerability may cause a denial-of-service condition or allow an attacker to gain the privileges of the sendmail daemon, typically root. Even vulnerable sendmail servers on the interior of a given network may be at risk since the vulnerability is triggered by the contents of a malicious email message.

III. Solution

Apply a patch from Sendmail Inc.

Sendmail has produced patches for versions 8.9, 8.10, 8.11, and 8.12. However, the vulnerability also exists in earlier versions of the code; therefore, site administrators using an earlier version are encouraged to upgrade to 8.12.9. These patches, and a signature file, are located at

ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu

ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu.asc

Apply a patch from your vendor

Many vendors include vulnerable sendmail servers as part of their software distributions. We have notified vendors of this vulnerability and recorded the statements they provided in Appendix A of this advisory. The most recent vendor information can be found in the systems affected section of VU#897604.

Enable the RunAsUser option

There is no known workaround for this vulnerability. Until a patch can be applied, you may wish to set the RunAsUser option to reduce the impact of this vulnerability. As a good general practice, the CERT/CC recommends limiting the privileges of an application or service whenever possible.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer Inc.

Apple has released Mac OS X 10.2.5 which includes the patch from the sendmail team for this vulnerability.

Conectiva

Conectiva Linux 6.0, 7.0 and 8 contain sendmail and are vulnerable to this issue, even though sendmail is no longer the default MTA in our distribution. Updated packages will be announced to our mailing lists when ready.

Cray

Cray Inc. may be vulnerable and has opened sprs 725085 and 725086 to investigate.

Hewlett-Packard

SOURCE: Hewlett-Packard Company HP Services Software Security Response Team

x-ref: SSRT3531 [HPSBUX0304-253, HPSBMP0304-018]

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products.

As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

Hitachi

HI-UX/WE2's sendmail is NOT Vulnerable to this issue.

IBM

The AIX operating system is vulnerable to sendmail buffer overflow attack mentioned in CERT Advisory CA-2003-12 and CERT Vulnerability Note VU# 897604.

An efix is available from:

ftp://ftp.software.ibm.com/aix/efixes/security/sendmail_2_efix.tar.Z

The APAR numbers and availability dated for this issue are as follows:

APAR number for AIX 4.3.3: IY42629 (available approx. 05/07/2003)
APAR number for AIX 5.1.0: IY42630 (available approx. 04/28/2003)
APAR number for AIX 5.2.0: IY42631 (available approx. 04/28/2003)

The APARs can be downloaded using the URL below and then following the links for your AIX release level.

http://techsupport.services.ibm.com/server/fixes?view=pSeries

For more information please contact your AIX Support Center.

Lotus

Lotus products are not vulnerable to this problem.

Mirapoint

Mirapoint has corrected this problem. Details of the update (D3_SMTP_CERT_2003_12) can be found on the Mirapoint secure support center.

Nortel Networks

The following Nortel Networks Wireless products are potentially affected by the vulnerabilities identified in CERT Advisory CA-2003-12:

- SS7 IP Gateway.
  Nortel Networks recommends disabling Sendmail as it is not used.
- Wireless Preside OAM&P Main Server.
  Sendmail should not be disabled on these products.

The following Nortel Networks Enterprise Voice IVR products are potentially affected by the vulnerabilities identified in CERT Advisory CA-2003-12:

- MPS1000
- MPS500
- VPS
- CTX

All the above products deploy Sendmail; it should not be disabled on these products.

For all of the above products Nortel Networks recommends applying the latest Sun Microsystems patches in accordance with that vendor's recommendations. To avoid applying patches twice, please ensure that the Sun Microsystems patch applied also addresses the vulnerability identified in CERT Advisory CA-2003-07.

The following Nortel Networks Succession products are potentially affected by the vulnerability identified in CERT Advisory CA-2003-12:

- SSPFS-based CS2000 Management Tools
- GWC Element Manager and QoS Collector Application (QCA)
- SAM21 Element Manager
- Audio Provisioning Server (APS) and APS client GUI
- UAS Element Manager
- Succession Media Gateway 9000 Element Manager (Mid-Tier and Server)
- Network Patch Manager (NPM)
- Nodes Configuration, Trunk Configuration, Carrier Endpoint Configuration, Lines Configuration (Servord+), Trunk Maintenance Manager, Lines Maintenance Manager, Line Test Manager, V5.2 Configuration and Maintenance, PM Poller, EMS Proxy Services, and Common Application Launch Point

A product bulletin will be issued shortly.

Sendmail has been disabled in SN06 and therefore SN06 is not vulnerable. A patch for SN05 is currently under development that will disable Sendmail in SN05 so that it will not be affected by the vulnerability identified in CERT Advisory CA-2003-12. The availability date for the SN05 patch is still to be determined.

For more information please contact Nortel at:

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/>

Red Hat Inc.

Red Hat distributes sendmail in all Red Hat Linux distributions. Updated sendmail packages that contain patches to correct this vulnerability are available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Linux:

http://rhn.redhat.com/errata/RHSA-2003-120.html

Red Hat Enterprise Linux:

http://rhn.redhat.com/errata/RHSA-2003-121.html

The Sendmail Consortium

The Sendmail Consortium recommends that sites upgrade to 8.12.9 whenever possible. Alternatively, patches are available for 8.9, 8.10, 8.11, and 8.12 on http://www.sendmail.org/.

Sendmail Inc.

All commercial releases including Sendmail Switch, Sendmail Advanced Message Server (which includes the Sendmail Switch MTA), Sendmail for NT, and Sendmail Pro are affected by this issue. Patch information is available at http://www.sendmail.com/security/.

Sequent (IBM)

For information please contact IBM Service at 1-800-IBM-SERV.

SGI

SGI acknowledges receiving CERT VU#897604 and is currently investigating. This is being tracked as SGI Bug# 886104. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported SGI operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on http://www.sgi.com/support/security/
[20030401-01-P]

Sun Microsystems Inc.

Solaris 2.6, 7, 8 and 9 are vulnerable to VU#897604.

Sun will be publishing a Sun Alert for the issue at the following location shortly:

http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/52620

The Sun Alert will be updated with the patch information as soon as the patches are available.

At that time, the patches listed in the Sun Alert will be available from:

http://sunsolve.sun.com/securitypatch

Wind River Systems Inc.

This vulnerability is addressed by the M500-008 patch for Platform for Server Appliances 1.0 or BSD/OS 5.0 based systems. The M31--005 patch addresses this problem for BSD/OS 4.3.1 or 4.3 systems, and the M420-034 addresses this problem for BSD/OS 4.2 based systems.

Our thanks to Eric Allman, Claus Assmann, Greg Shapiro, and Dave Anderson of Sendmail for reporting this problem and for their assistance in coordinating the response to this problem. We also thank Michal Zalewski for discovering this vulnerability.

Authors: Art Manion, Shawn V. Hernan, and Jeffery P. Lanza.

Revision History

March 29, 2003: Initial release

March 29, 2003: Added Conectiva statement, reformated vendor statements

March 30, 2003: Added Wind River Systems and HP vendor statements

March 31, 2003: Added Sun, IBM, SGI, and Cray vendor statements

April 1, 2003: Added Apple and Lotus vendor statements, updated Red Hat and IBM statements

April 7, 2003: Updated SGI and HP statements

April 8, 2003: Added Nortel statement

April 11, 2003: Updated Apple statement

April 15, 2003: Updated HP statement

April 22, 2003: Added Mirapoint statement

April 29, 2003: Added Sequent (IBM) statement

May 20, 2003: Added Hitachi statement

May 29, 2003: Updated description

13 CA-2003-13: Multiple Vulnerabilities in Snort Preprocessors

Original release date: April 17, 2003
Last revised: April 23, 2003
Source: CERT/CC

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

Systems Affected

- For VU#139129: Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1.
- For VU#916785: Snort versions 1.8.x through 1.9.0 and 2.0 Beta.

Overview

There are two vulnerabilities in the Snort Intrusion Detection System, each in a separate preprocessor module. Both vulnerabilities allow remote attackers to execute arbitrary code with the privileges of the user running Snort, typically root.

I. Description

The Snort intrusion detection system ships with a variety of preprocessor modules that allow the user to selectively include additional functionality. Researchers from two independent organizations have discovered vulnerabilities in two of these modules, the RPC preprocessor and the "stream4" TCP fragment reassembly preprocessor.

For additional information regarding Snort, please see http://www.snort.org/.

VU#139129 - Heap overflow in Snort "stream4" preprocessor (CAN-2003-0209)

Researchers at CORE Security Technologies have discovered a remotely exploitable heap overflow in the Snort "stream4" preprocessor module. This module allows Snort to reassemble TCP packet fragments for further analysis.

To exploit this vulnerability, an attacker must disrupt the state tracking mechanism of the preprocessor module by sending a series of packets with crafted sequence numbers. This causes the module to bypass a check for buffer overflow attempts and allows the attacker to insert arbitrary code into the heap.

For additional information, please read the Core Security Technologies Advisory located at

http://www.coresecurity.com/common/showdoc.php?idx=313&idxseccion=10

This vulnerability affects Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1, including Snort 1.9.1. Snort has published an advisory regarding this vulnerability; it is available at http://www.snort.org/advisories/snort-2003-04-16-1.txt.

VU#916785 - Buffer overflow in Snort RPC preprocessor (CAN-2003-0033)

Researchers at Internet Security Systems (ISS) have discovered a remotely exploitable buffer overflow in the Snort RPC preprocessor module. Martin Roesch, primary developer for Snort, described the vulnerability as follows:

When the RPC decoder normalizes fragmented RPC records, it incorrectly checks the lengths of what is being normalized against the current packet size, leading to an overflow condition. The RPC preprocessor is enabled by default.

For additional information, please read the ISS X-Force advisory located at

http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21951

This vulnerability affects Snort versions 1.8.x through 1.9.0 and 2.0 Beta. Snort version 1.9.1 is not affected.

II. Impact

Both VU#139129 and VU#916785 allow remote attackers to execute arbitrary code with the privileges of the user running Snort, typically root. Please note that it is not necessary for the attacker to know the IP address of the Snort device they wish to attack; merely sending malicious traffic where it can be observed by an affected Snort sensor is sufficient to exploit these vulnerabilities.

III. Solution

Upgrade to Snort 2.0

Both VU#139129 and VU#916785 are addressed in Snort version 2.0, which is available at

http://www.snort.org/dl/snort-2.0.0.tar.gz

Binary-only versions of Snort are available from

http://www.snort.org/dl/binaries

For information from other vendors that ship affected versions of Snort, please see Appendix A of this document.

Disable affected preprocessor modules

Sites that are unable to immediately upgrade affected Snort sensors may prevent exploitation of this vulnerability by commenting out the affected preprocessor modules in the "snort.conf" configuration file.

To prevent exploitation of VU#139129, comment out the following line:

```
preprocessor stream4_reassemble
```

To prevent exploitation of VU#916785, comment out the following line:

```
preprocessor rpc_decode: 111 32771
```

After commenting out the affected modules, send a SIGHUP signal to the affected Snort process to update the configuration. Note that disabling these modules may have adverse effects on a sensor's ability to correctly process RPC record fragments and TCP packet fragments. In particular, disabling the "stream4" preprocessor module will prevent the Snort sensor from detecting a variety of IDS evasion attacks.

Block outbound packets from Snort IDS systems

You may be able limit an attacker's capabilities if the system is compromised by blocking all outbound traffic from the Snort sensor. While this workaround will not prevent exploitation of the vulnerability, it may make it more difficult for the attacker to create a useful exploit.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Snort is not shipped with Mac OS X or Mac OS X Server.

Ingrian Networks

Ingrian Networks products are not susceptible to VU#139129 and VU#916785 since they do not use Snort.

Ingrian customers who are using the IDS Extender Service Engine to mirror cleartext data to a Snort-based IDS should upgrade their IDS software.

NetBSD

NetBSD does not include snort in the base system.

Snort is available from the 3rd party software system, pkgsrc. Users who have installed net/snort, net/snort-mysql or net/snort-pgsql should update to a fixed version. pkgsrc/security/audit-packages can be used to keep up to date with these types of issues.

Red Hat Inc.

Not vulnerable. Red Hat does not ship Snort in any of our supported products.

SGI

SGI does not ship snort as part of IRIX.

Snort

Snort 2.0 has undergone an external third party professional security audit funded by Sourcefire.

The CERT/CC acknowledges Bruce Leidl, Juan Pablo Martinez Kuhn, and Alejandro David Weil of Core Security Technologies for their discovery of VU#139129. We also acknowledge Mark Dowd and Neel Mehta of ISS X-Force for their discovery of VU#916785.

Authors: Jeffrey P. Lanza and Cory F. Cohen.

Revision History

```
Apr 17, 2003: Initial release

Apr 17, 2003: Fixed CVE candidate reference for VU#139129; now reads
"CAN-2003-0209"

Apr 17, 2003: Minor grammar changes in Impact section

Apr 22, 2003: Fixed spelling error in Solution section

Apr 23, 2003: Revised Systems Affected section

Apr 23, 2003: Revised systems affected information in Description
section
```

14 CA-2003-14: Buffer Overflow in Microsoft Windows HTML Conversion Library

Original issue date: July 14, 2003
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Windows 98 and 98 Second Edition (SE)
- Windows NT 4.0 and 4.0 Terminal Server Edition (TSE)
- Windows Millennium Edition (Me)
- Windows 2000
- Windows XP
- Windows Server 2003

Overview

A buffer overflow vulnerability exists in a shared HTML conversion library included in Microsoft Windows. An attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

I. Description

Microsoft Windows includes a shared HTML conversion library (`html32.cnv`). According to Microsoft Security Bulletin MS03-023, "The HTML converter is an extension which allows applications to convert HTML data into Rich Text Format (RTF) while maintaining the formatting and structure of the data as well as the text. The converter also supports the conversion of RTF data into HTML."

The HTML conversion library contains a buffer overflow vulnerability that can be triggered by a specially crafted *align* attribute in an <HR> element. The library can be loaded by any application on the system. For example, Internet Explorer (IE) uses the library to handle HTML data stored in the clipboard. Using script, an attacker can cause IE to copy a crafted <HR> element into the clipboard and load the library. The attacker could accomplish this by convincing a victim to view an HTML web page or HTML email message with IE, Outlook, or Outlook Express in a zone where *Active scripting* and *Allow paste operations via script* are enabled.

This vulnerability is not limited to IE, Outlook, or Outlook Express. Any program, including non-Microsoft applications, can use the vulnerable library and may present other vectors of attack.

Further information is available in VU#823260. Common Vulnerabilities and Exposures (CVE) refers to this issue as CAN-2003-0469.

II. Impact

An attacker could execute arbitrary code with the privileges of the process that loaded the HTML conversion library. The attacker could also crash the process, causing a denial of service.

III. Solution

Apply a patch

Apply the appropriate patch as specified by Microsoft Security Bulletin MS03-023.

Modify Internet Explorer security zone configuration

Modify one or both of the following IE security zone settings in the Internet zone and the zone(s) used by Outlook, Outlook Express, and any other application that uses Internet Explorer or the WebBrowser ActiveX control to render HTML:

- Set *Allow paste operations via script* to *Disable*
- Set *Active scripting* to *Disable*

Either of these changes will prevent attacks that depend on scripting in the IE HTML rendering engine. However, these changes are not complete solutions, and they do not prevent attacks that use other vectors.

Note that disabling *Active scripting* provides defense against other attacks that are outside the scope of this document.

Instructions for modifying IE 5 security zone settings can be found in the CERT/CC Malicious Web Scripts FAQ. In IE 6, the *High* security zone setting includes both of these changes.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS03-023.

Appendix B References

- CERT/CC Vulnerability Note VU#823260 - http://www.kb.cert.org/vuls/id/823260
- Microsoft Security Bulletin MS03-023 - http://microsoft.com/technet/security/bulletin/MS03-023.asp

This vulnerability was publicly reported by Digital Scream.

Feedback can be directed to the author, Art Manion.

Revision History

July 14, 2003: Initial release

15 CA-2003-15: Cisco IOS Interface Blocked by IPv4 Packet

Original release date: July 16, 2003
Last revised: July 17, 2003
Source: CERT/CC

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

Systems Affected

- All Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets

Overview

A vulnerability in many versions of Cisco IOS could allow an intruder to execute a denial-of-service attack against a vulnerable device.

I. Description

Cisco IOS is a very widely deployed network operating system. A vulnerability in IOS could allow an intruder to execute a denial-of-service attack against an affected device. Cisco has published an advisory on this topic, available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

We strongly encourage sites using IOS to read this document and take appropriate action.

The CERT/CC is tracking this issue as VU#411332. This reference number corresponds to CVE candidate CAN-2003-0567.

II. Impact

By sending specially crafted IPv4 packets to an interface on a vulnerable device, an intruder can cause the device to stop processing packets destined to that interface. Quoting from Cisco's advisory:

A device receiving these specifically crafted IPv4 packets will force the inbound interface to stop processing traffic. The device may stop processing packets destined to the router, including routing protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct itself. This issue can affect all Cisco devices running Cisco IOS software. This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.

III. Solution

Apply a patch from Cisco

Apply a patch as described in Cisco's Advisory.

Restrict access

Until a patch can be applied, you can mitigate the risks presented by this vulnerability by judicious use of access control lists (ACLs). The correct use of ACLs depends on your network topology. Additionally, ACLs may degrade performance on some systems. We recommend reviewing the following before applying ACLs:

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml#workarounds
http://www.cisco.com/warp/public/707/racl.html
http://www.cisco.com/warp/public/707/iacl.html

The CERT Coordination Center thanks Cisco Systems for notifying us about this problem and for helping us to construct this advisory.

Feedback about this advisory may be directed to the author, Shawn Hernan.

Revision History

```
July 16, 2003: Initial release
```

```
July 17, 2003: Minor formatting changes
```

16 CA-2003-16: Buffer Overflow in Microsoft RPC

Original release date: July 17, 2003
Last revised: Fri Aug 8 13:11 EDT 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0 Terminal Services Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Overview

A buffer overflow vulnerability exists in Microsoft's Remote Procedure Call (RPC) implementation. A remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

I. Description

There is a buffer overflow in Microsoft's RPC implementation. According to Microsoft Security Bulletin MS03-026, "There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on TCP/IP port 135. This interface handles DCOM object activation requests that are sent by client machines (such as Universal Naming Convention (UNC) paths) to the server."

The CERT/CC is tracking this issue as VU#568148. This reference number corresponds to CVE candidate CAN-2003-0352.

II. Impact

A remote attacker could exploit this vulnerability to execute arbitrary code with Local System privileges or to cause a denial of service.

III. Solution

Apply a patch from your vendor

Apply the appropriate patch as specified by >Microsoft Security Bulletin MS03-026.

Appendix A contains additional information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments. Please contact your vendor directly.

Restrict access

You may wish to block access from outside your network perimeter, specifically by blocking access to TCP & UDP ports 135, 139, and 445. This will limit your exposure to attacks. However, blocking at the network perimeter would still allow attackers within the perimeter of your network to exploit the vulnerability. It is important to understand your network's configuration and service requirements before deciding what changes are appropriate.

Disable DCOM

Depending on site requirements, you may wish to disable DCOM as described in MS03-026. Disabling DCOM will help protect against this vulnerability, but may also cause undesirable side effects. Additional details on disabling DCOM and possible side effects are available in Microsoft Knowledge Base Article 825750.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments.

Microsoft Corporation

Apply the appropriate patch as specified by Microsoft Security Bulletin MS03-026.

Nortel Networks

Nortel Networks Response to CERT Advisory CA-2003-16 - *Buffer Overflow in Microsoft RPC*

Nortel Networks supplies and supports both integrated and non-integrated solutions to its customers. We are taking this opportunity to complement CERT and Microsoft information with information specific to the potential impact of this vulnerability on Nortel Networks products and solutions. As well we indicate how Nortel Networks products can be used to help effect the mitigation procedures recommended both by CERT and Microsoft.

A limited number of Nortel Networks products and solutions are potentially affected by this issue, and the nature of these products and solutions tends to place them within a private network. Accordingly, if network perimeter protection is employed as recommended by both CERT and Microsoft (i.e. blocking access to TCP & UDP ports 135, 139, and 445) these products and solutions should not be vulnerable to attacks from the public Internet.

Nortel Networks would like to inform its customers and partners of efforts currently under way to respond to this issue:

1. *Embedded Operating Systems*

   Some Nortel Networks products employ embedded Windows Operating Systems identified by Microsoft as vulnerable; Product Technical Bulletins and patches are being developed.

2. *Applications on Windows Operating Systems*

   Some Nortel Networks applications reside on Windows Operating Systems identified by Microsoft as vulnerable; the corresponding Microsoft patches are being tested against the Nortel Networks applications to confirm that their functionality will not be impacted.

3. *Clients on Windows Operating Systems*

   Some Nortel Networks clients reside on workstations supplied by others, with Windows Operating Systems identified by Microsoft as vulnerable; Nortel Networks recommends that customers follow the recommendations of CERT and Microsoft and apply the appropriate patches.

4. *Nortel Networks Routing Products to be used for Port Blocking*

   Nortel Networks routing products are not vulnerable to this issue, but may be configured to protect customer networks by blocking access to TCP & UDP ports 135, 139, and 445 at the network edge, as recommended by CERT and Microsoft. Product-specific instructions for port blocking configuration are available for the following Nortel products:

- Passport 6000
- Shasta
- Contivity
- Alteon Switched Firewall
- Passport 8600
- BayRS

Nortel Networks Product Status

The following products, which in some way rely on a Microsoft operating system, have been reviewed or are under review. Other products may be added.

Not Vulnerable

- Succession Multi-service Gateway 4000
- Interactive Multimedia Server
- Communication Server for Enterprise -- Multimedia Exchange
- Multimedia PC Client
- Optivity Telephony Manager
- Optivity NetID
- Optivity Policy Services
- Optivity Switch Manager
- Contivity Configuration Manager

Vulnerable

- Symposium including TAPI ICM
- CallPilot
- Business Communications Manager
- International Centrex-IP
- Periphonics with OSCAR Speech Server

Under Review

- Alteon Security Manager
- Network Configuration Manager for BCM
- Preside Site Manager
- Preside System Manager Interface

If you have a Nortel Networks product which is not noted on the list above, we are currently reviewing our extended product families to identify if they use components of the Microsoft Operating System and will issue an updated list as soon as new information is available.

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*.

This vulnerability was discovered by The Last Stage of Delirium Research Group. Microsoft has published Microsoft Security Bulletin MS03-026, upon which this document is largely based.

Author: Ian A. Finlay

Revision History

Jul 17, 2003: Initial release

Jul 21, 2003: Revised Restrict access in Solution section to add additional ports to block

Aug 2, 2003: Added Appendix A Vendor Information

Aug 2, 2003: Added Nortel Vendor Statement from 08/01/2003

Aug 8, 2003: Added Disable DCOM workaround to Solution section.

17 CA-2003-17: Exploit Available for the Cisco IOS Interface Blocked Vulnerabilities

Original release date: July 18, 2003
Last revised: --
Source: CERT/CC

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

Systems Affected

- All Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets

Overview

An exploit has been posted publicly for the vulnerability described in VU#411332, which was announced in http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

I. Description

An exploit has been posted publicly for VU#411332. This exploit allows an attacker to interrupt the normal operation of a vulnerable device. We believe it is likely that intruders will begin using this or other exploits to cause service outages.

Many large service providers have already taken action or are in the midst of upgrading. However, if you have not already taken action, we strongly encourage you to review the advisory provided by Cisco and take action in accordance with your site's maintenance and change management procedures. Cisco's advisory can be found at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

The CERT/CC will continue to provide information about this vulnerability through VU#411332.

Any information regarding intruder activity related to this vulnerability will be posted to the CERT/CC Currect Activity page, available at

http://www.cert.org/current/

II. Impact

By sending specially crafted IPv4 packets to an interface on a vulnerable device, an intruder can cause the device to stop processing packets destined to that interface. Quoting from Cisco's advisory:

> *A device receiving these specifically crafted IPv4 packets will force the inbound interface to stop processing traffic. The device may stop processing packets destined to the router, including routing protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct itself. This issue can affect all Cisco devices running Cisco IOS software. This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.*

III. Solution

Apply a patch from Cisco

Upgrade as described in Cisco's Advisory.

Restrict access

Until a patch can be applied, you can mitigate the risks presented by this vulnerability by judicious use of access control lists (ACLs). The correct use of ACLs depends on your network topology. Additionally, ACLs may degrade performance on some systems. We recommend reviewing the following before applying ACLs:

> http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml#workarounds
> http://www.cisco.com/warp/public/707/racl.html
> http://www.cisco.com/warp/public/707/iacl.html

The CERT Coordination Center thanks Cisco Systems for notifying us about this problem and for helping us to construct this advisory.

Authors: Shawn Hernan and Martin Lindner

Revision History

```
July 18, 2003: Initial release
```

18 CA-2003-18: Integer Overflows in Microsoft Windows DirectX MIDI Library

Original issue date: July 25, 2003
Last revised: July 30, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows systems running DirectX (Windows 98, 98SE, NT 4.0, NT 4.0 TSE, 2000, XP, Server 2003)

Overview

A set of integer overflows exists in a DirectX library included in Microsoft Windows. An attacker could exploit these vulnerabilities to execute arbitrary code or to cause a denial of service.

I. Description

Microsoft Windows operating systems include multimedia technologies called DirectX and DirectShow. From Microsoft Security Bulletin MS03-030, "DirectX consists of a set of low-level Application Programming Interfaces (APIs) that are used by Windows programs for multimedia support. Within DirectX, the DirectShow technology performs client-side audio and video sourcing, manipulation, and rendering."

DirectShow support for MIDI files is implemented in a library called `quartz.dll`. This library contains two vulnerabilities:

VU#561284 - Microsoft Windows DirectX MIDI library does not adequately validate Text or Copyright parameters in MIDI files

VU#265232 - Microsoft Windows DirectX MIDI library does not adequately validate MThd track values in MIDI files

In both cases, a specially crafted MIDI file could cause an integer overflow, leading to incorrect memory allocation and heap corruption.

Any application that uses DirectX/DirectShow to process MIDI files may be affected by these vulnerabilities. Of particular concern, Internet Explorer (IE) uses the Windows Media Player ActiveX control and `quartz.dll` to handle MIDI files embedded in HTML documents. An attacker could therefore exploit these vulnerabilities by convincing a victim to view an HTML document, such as a web page or an HTML email message, that contains an embedded MIDI file.

Note that in addition to IE, a number of applications, including Outlook, Outlook Express, Eudora, AOL, Lotus Notes, and Adobe PhotoDeluxe, use the WebBrowser ActiveX control to interpret HTML documents.

Further technical details are available in eEye Digital Security advisory AD20030723. Common Vulnerabilities and Exposures (CVE) refers to these vulnerabilities as CAN-2003-0346.

II. Impact

By convincing a victim to access a specially crafted MIDI or HTML file, an attacker could execute arbitrary code with the privileges of the victim. The attacker could also cause a denial of service in any application that uses the vulnerable functions in `quartz.dll`.

III. Solution

Apply a patch

Apply the appropriate patch as specified by Microsoft Security Bulletin MS03-030.

The patch is a complete solution that fixes the integer overflows in `quartz.dll`. Sites that are unable to install the patch may consider the workaround described below.

Modify Internet Explorer settings

It is possible to significantly limit the ability of IE to automatically load MIDI files from HTML documents by making all of the following modifications:

- Disable *Active scripting*
- Disable *Run ActiveX controls and plug-ins*
- Disable *Play sounds in web pages*
- Disable *Play videos in web pages*

As stated above, the only complete solution for these vulnerabilities is to apply the patch. For example, Outlook Express 6 SP1 will play a MIDI file in an HTML email message regardless of the settings for audio and video in web pages. There may be other methods to automatically load a MIDI file from an HTML document. Also, these modifications will prevent some web pages from functioning properly.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS03-030.

Appendix B References

- CERT/CC Vulnerability Note VU#561284 - http://www.kb.cert.org/vuls/id/561284
- CERT/CC Vulnerability Note VU#265232 - http://www.kb.cert.org/vuls/id/265232
- eEye Digital Security advisory AD20030723 - http://www.eeye.com/html/Research/Advisories/AD20030723.html
- Microsoft Security Bulletin MS03-030 - http://microsoft.com/technet/security/bulletin/MS03-030.asp
- Microsoft Knowledge Base article 819696 - http://support.microsoft.com/default.aspx?scid=kb;en-us;819696

These vulnerabilities were researched and reported by eEye Digital Security. Jeff Johnson helped research the IE settings workaround.

Feedback can be directed to the author, Art Manion.

Revision History

July 25, 2003: Initial release, added Windows XP to Systems Affected

July 29, 2003: Removed IE security settings workaround from Solution

July 30, 2003: Updated IE settings workaround in Solution, changed references to vulnerabilities (plural), updated credits

19 CA-2003-19: Exploitation of Vulnerabilities in Microsoft RPC Interface

Original issue date: July 31, 2003
Last revised: July 31, 2003 21:25 UTC-0400
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0 Terminal Services Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Overview

The CERT/CC is receiving reports of widespread scanning and exploitation of two recently discovered vulnerabilities in Microsoft Remote Procedure Call (RPC) Interface.

I. Description

Reports to the CERT/CC indicate that intruders are actively scanning for and exploiting a vulnerability in Microsoft's DCOM RPC interface as described in VU#568148 and CA-2003-16. Multiple exploits for this vulnerability have been publicly released, and there is active development of improved and automated exploit tools for this vulnerability. Known exploits target TCP port 135 and create a privileged backdoor command shell on successfully compromised hosts. Some versions of the exploit use TCP port 4444 for the backdoor, and other versions use a TCP port number specified by the intruder at run-time. We have also received reports of scanning activity for common backdoor ports such as 4444/TCP. In some cases, due to the RPC service terminating, a compromised system may reboot after the backdoor is accessed by an intruder.

There appears to be a separate denial-of-service vulnerability in Microsoft's RPC interface that is also being targeted. Based on current information, we believe this vulnerability is separate and independent from the RPC vulnerability addressed in MS03-026. The CERT/CC is tracking this additional vulnerability as VU#326746 and is continuing to work to understand the issue and mitigation strategies. Exploit code for this vulnerability has been publicly released and also targets TCP port 135.

In both of the attacks described above, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies.

II. Impact

A remote attacker could exploit these vulnerabilities to execute arbitrary code with Local System privileges or to cause a denial of service condition.

III. Solutions

Apply patches

All users are encouraged to apply the patches referred to in Microsoft Security Bulletin MS03-026 as soon as possible in order to mitigate the vulnerability described in VU#568148. These patches are also available via Microsoft's Windows Update service.

Systems running Windows 2000 may still be vulnerable to at least a denial of service attack via VU#326746 if their DCOM RPC service is available via the network. Therefore, sites are encouraged to use the packet filtering tips below in addition to applying the patches supplied in MS03-026.

Filter network traffic

Sites are encouraged to block network access to the RPC service at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include

- 135/TCP
- 135/UDP
- 139/TCP
- 139/UDP
- 445/TCP
- 445/UDP

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

Because current exploits for VU#568148 create a backdoor, which is in some cases 4444/TCP, blocking inbound TCP sessions to ports on which no legitimate services are provided may limit intruder access to compromised hosts.

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

Reporting

The CERT/CC is tracking activity related to exploitation of the first vulnerability (VU#568148) as CERT#27479 and the second vulnerability (VU#326746) as CERT#24523. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS03-026.

Appendix B References

- CERT/CC Vulnerability Note VU#561284 - http://www.kb.cert.org/vuls/id/561284
- CERT/CC Vulnerability Note VU#326746 - http://www.kb.cert.org/vuls/id/326746
- Microsoft Security Bulletin MS03-026 - http://microsoft.com/technet/security/bulletin/MS03-026.asp
- Microsoft Knowledge Base article 823980 - http://support.microsoft.com?kbid=823980

Authors: Chad Dougherty and Kevin Houle

Revision History

July 31, 2003: Initial release July 31, 2003: Fixed HREF in References section

20 CA-2003-20: W32/Blaster worm

Original issue date: August 11, 2003
Last revised: August 14, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Overview

The CERT/CC is receiving reports of widespread activity related to a new piece of malicious code known as W32/Blaster. This worm appears to exploit known vulnerabilities in the Microsoft Remote Procedure Call (RPC) Interface.

I. Description

The W32/Blaster worm exploits a vulnerability in Microsoft's DCOM RPC interface as described in VU#568148 and CA-2003-16. Upon successful execution, the worm attempts to retrieve a copy of the file `msblast.exe` from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies. Microsoft has published information about this vulnerability in Microsoft Security Bulletin MS03-026.

Lab testing has confirmed that the worm includes the ability to launch a TCP SYN flood denial-of-service attack against windowsupdate.com. We are investigating the conditions under which this attack might manifest itself. Unusual or unexpected traffic to windowsupdate.com may indicate an infection on your network, so you may wish to monitor network traffic.

Sites that do not use windowsupdate.com to manage patches may wish to block outbound traffic to windowsupdate.com. In practice, this may be difficult to achieve, since windowsupdate.com may not resolve to the same address every time. Correctly blocking traffic to windowsupdate.com will require detailed understanding of your network routing architecture, system management needs, and name resolution environment. You should not block traffic to windowsupdate.com without a thorough understanding of your operational needs.

We have been in contact with Microsoft regarding this possibility of this denial-of-service attack.

II. Impact

A remote attacker could exploit these vulnerabilities to execute arbitrary code with Local System privileges or to cause a denial-of-service condition.

III. Solutions

(NOTE: Detailed instructions for recovering Windows XP systems from the W32/Blaster worm can be found in the W32/Blaster Recovery Tech Tip)

Apply patches

All users are encouraged to apply the patches referred to in Microsoft Security Bulletin MS03-026 as soon as possible in order to mitigate the vulnerability described in VU#568148. These patches are also available via Microsoft's Windows Update service.

Systems running Windows 2000 may still be vulnerable to at least a denial-of-service attack via VU#326746 if their DCOM RPC service is available via the network. Therefore, sites are encouraged to use the packet filtering tips below in addition to applying the patches supplied in MS03-026.

It has been reported that some affected machines are not able to stay connected to the network long enough to download patches from Microsoft. For hosts in this situation, the CERT/CC recommends the following:

1. Physically disconnect the system from the network.
2. Check the system for signs of compromise.
   - In most cases, an infection will be indicated by the presence of the registry key `"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update"` with a value of `msblast.exe`. Other possible values include `teekids.exe` and `penis32.exe`. If this key is present, remove it using a registry editor.
3. If you're infected, terminate the running copy of `msblast.exe`, `teekids.exe` or `penis32.exe` using the Task Manager.
4. Search for and delete files named `msblast.exe`, `teekids.exe` or `penis32.exe`.
5. Take one of the following steps to protect against the compromise prior to installing the Microsoft patch:
   - Disable DCOM as described in MS03-026 and Microsoft Knowledge Base Article 825750.
   - Enable Microsoft's Internet Connection Firewall (ICF) or another host-level packet filtering program to block incoming connections to port 135/TCP. Information about ICF is available in Microsoft Knowledge Base Article 283673.
6. Reconnect the system to the network and apply the patches referenced in MS03-026.

Trend Micro, Inc. has published a set of steps to accomplish these goals. Symantec has also published a set of steps to accomplish these goals.

Disable DCOM

Depending on site requirements, you may wish to disable DCOM as described in MS03-026. Disabling DCOM will help protect against this vulnerability but may also cause undesirable side effects. Additional details on disabling DCOM and possible side effects are available in Microsoft Knowledge Base Article 825750.

Filter network traffic

Sites are encouraged to block network access to the following relevant ports at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include

- 69/UDP
- 135/TCP
- 135/UDP
- 139/TCP
- 139/UDP
- 445/TCP
- 445/UDP
- 593/TCP
- 4444/TCP

Sites should consider blocking both inbound *and* outbound traffic to these ports, depending on network requirements, at the host and network level. Microsoft's Internet Connection Firewall can be used to accomplish these goals.

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

Because current exploits for VU#568148 create a backdoor, which is in some cases 4444/TCP, blocking inbound TCP sessions to ports on which no legitimate services are provided may limit intruder access to compromised hosts.

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

Reporting

The CERT/CC is tracking activity related to this worm as CERT#30479. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS03-026.

Appendix B References

- CERT/CC Advisory CA-2003-19 - http://www.cert.org/advisories/CA-2003-19.html
- CERT/CC Vulnerability Note VU#561284 - http://www.kb.cert.org/vuls/id/561284
- CERT/CC Vulnerability Note VU#326746 - http://www.kb.cert.org/vuls/id/326746
- Microsoft Security Bulletin MS03-026 - http://microsoft.com/technet/security/bulletin/MS03-026.asp
- Microsoft Knowledge Base article 823980 - http://support.microsoft.com?kbid=823980

Thanks

Our thanks to Microsoft Corporation for their review of and input to this advisory.

Authors: Chad Dougherty, Jeffrey Havrilla, Shawn Hernan, and Marty Lindner

Revision History

August 11, 2003: Initial release

August 12, 2003: Updated recovery steps

August 12, 2003: Added link to the W32/Blaster Tech Tip

August 13, 2003: Added filenames of known variants to removal instructions

August 14, 2003: Added port to filter (593/TCP)

21 CA-2003-21: GNU Project FTP Server Compromise

Original issue date: August 13, 2003
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Overview

The CERT/CC has received a report that the system housing the primary FTP servers for the GNU software project was compromised.

I. Description

The GNU Project, principally sponsored by the Free Software Foundation (FSF), produces a variety of freely available software. The CERT/CC has learned that the system housing the primary FTP servers for the GNU software project, `gnuftp.gnu.org`, was root compromised by an intruder. The more common host names of `ftp.gnu.org` and `alpha.gnu.org` are aliases for the same compromised system. The compromise is reported to have occurred in March of 2003.

The FSF has released an announcement describing the incident.

Because this system serves as a centralized archive of popular software, the insertion of malicious code into the distributed software is a serious threat. As the above announcement indicates, however, no source code distributions are believed to have been maliciously modified at this time.

II. Impact

The potential exists for an intruder to have inserted back doors, Trojan horses, or other malicious code into the source code distributions of software housed on the compromised system.

III. Solution

We encourage sites using the GNU software obtained from the compromised system to verify the integrity of their distribution.

Sites that mirror the source code are encouraged to verify the integrity of their sources. We also encourage users to inspect any and all other software that may have been downloaded from the compromised site. Note that it is not always sufficient to rely on the timestamps or file sizes when trying to determine whether or not a copy of the file has been modified.

Verifying checksums

The FSF has produced PGP-signed lists of known-good MD5 hashes of the software packages housed on the compromised server. These lists can be found at

ftp://ftp.gnu.org/before-2003-08-01.md5sums.asc

ftp://alpha.gnu.org/before-2003-08-01.md5sums.asc

Note that both of these files and the announcement above are signed by Bradley Kuhn, Executive Director of the FSF, with the following PGP key:

```
pub 1024D/DB41B387 1999-12-09 Bradley M. Kuhn <bkuhn@fsf.org>

 Key fingerprint = 4F40 645E 46BE 0131 48F9 92F6 E775 E324 DB41 B387

uid Bradley M. Kuhn (bkuhn99) <bkuhn@ebb.org>

uid Bradley M. Kuhn <bkuhn@gnu.org>

sub 2048g/75CA9CB3 1999-12-09
```

The CERT/CC believes this key to be valid.

As a matter of good security practice, the CERT/CC encourages users to verify, whenever possible, the integrity of downloaded software. For more information, see IN-2001-06.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Free Software Foundation

```
 The current files on alpha.gnu.org and ftp.gnu.org as of 2003-08-02 have

 all been verified, and their md5sums and the reasons we believe the

 md5sums can be trusted are in:

 ftp://ftp.gnu.org/before-2003-08-01.md5sums.asc

 ftp://alpha.gnu.org/before-2003-08-01.md5sums.asc

 We are updating that file and the site as we confirm good md5sums of

 additional files. It is theoretically possible that downloads between
 March 2003 and July 2003 might have been source-compromised, so we
 encourage everyone to re-download sources and compare with the current
 copies for files on the site.
```

Appendix B References

- FSF announcement regarding the incident - ftp://ftp.gnu.org/MISSING-FILES.README
- CERT Incident Note IN-2001-06 - http://www.cert.org/incident_notes/IN-2001-06.html

The CERT/CC thanks Bradley Kuhn and Brett Smith of the Free Software Foundation for their timely assistance in this matter.

Feedback can be directed to the author: Chad Dougherty.

This document is available from: http://www.cert.org/advisories/CA-2003-21.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/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

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

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

```
August 13, 2003: Initial release
```

22 CA-2003-22: Multiple Vulnerabilities in Microsoft Internet Explorer

Original issue date: August 26, 2003
Last revised: October 6, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

Microsoft Windows systems running

- Internet Explorer 5.01
- Internet Explorer 5.50
- Internet Explorer 6.01

Previous, unsupported versions of Internet Explorer may also be affected.

Overview

Microsoft Internet Explorer (IE) contains multiple vulnerabilities, the most serious of which could allow a remote attacker to execute arbitrary code with the privileges of the user running IE.

Note: (2003-10-04) The patch provided by MS03-032 does not completely resolve the vulnerability described in VU#865940. Microsoft has since released MS03-040 which supercedes MS03-032.

I. Description

Microsoft Security Bulletin MS03-032 describes five vulnerabilities in Internet Explorer. These vulnerabilities are listed below. More detailed information is available in the individual vulnerability notes. Note that in addition to IE, any applications that use the IE HTML rendering engine to interpret HTML documents may present additional attack vectors for these vulnerabilities.

VU#205148 - Microsoft Internet Explorer does not properly evaluate Content-Type and Content-Disposition headers
A cross-domain scripting vulnerability exists in the way IE evaluates Content-Type and Content-Disposition headers and checks for files in the local browser cache. This vulnerability could allow a remote attacker to execute arbitrary script in a different domain, including the Local Machine Zone.

(Other resources: SNS Advisory No.67, CAN-2003-0531)

VU#865940 - Microsoft Internet Explorer does not properly evaluate "application/hta" MIME type referenced by DATA attribute of OBJECT element

IE will execute an HTML Application (HTA) referenced by the DATA attribute of an OBJECT element if the Content-Type header returned by the web server is set to "application/hta". An attacker could exploit this vulnerability to execute arbitrary code with the privileges of the user running IE.

(Other resources: eEye Digital Security Advisory AD20030820, MS03-032, MS02-040, CAN-2003-0532, CAN-2003-0838, CAN-2003-0809)

VU#548964 - Microsoft Windows BR549.DLL ActiveX control contains vulnerability
The Microsoft Windows BR549.DLL ActiveX control, which provides support for the Windows Reporting Tool, contains an unknown vulnerability. The impact of this vulnerability is not known.

VU#813208 - Microsoft Internet Explorer does not properly render an input type tag
IE does not properly render an input type tag, allowing a remote attacker to cause a denial of service.

VU#334928 - Microsoft Internet Explorer contains buffer overflow in Type attribute of OBJECT element on double-byte character set systems
Certain versions of IE that support double-byte character sets (DBCS) contain a buffer overflow vulnerability in the Type attribute of the OBJECT element. A remote attacker could execute arbitrary code with the privileges of the user running IE.

(Other resources: SNS Advisory No.68, Microsoft Security Bulletin MS03-020, CAN-2003-0344)

II. Impact

These vulnerabilities have different impacts, ranging from denial of service to execution of arbitrary commands or code. Please see the individual vulnerability notes for specific information. The most serious of these vulnerabilities (VU#865940) could allow a remote attacker to execute arbitrary code with the privileges of the user running IE. The attacker could exploit this vulnerability by convincing the user to access a specially crafted HTML document, such as a web page or HTML email message. No user intervention is required beyond viewing the attacker's HTML document with IE.

III. Solution

Apply a patch

Apply the appropriate patch as specified by Microsoft Security Bulletin MS03-040.

Note: (2003-10-04) The patch described in MS03-032 (822925) does not completely resolve the vulnerability described in VU#865940. This patch does not address at least two attack vectors that can be used to exploit this vulnerability. Microsoft has since released Security Bulletin MS03-040 which supercedes MS03-032 and addresses the other attack vectors for VU#865940. The CERT/CC encourages users to apply the patch referenced in MS03-040 and also consider applying the additional steps listed in the solution section of VU#865940.

The patch also changes the behavior of the HTML Help system (see VU#25249):

> *As with the previous Internet Explorer cumulative patches released with bulletins MS03-004, MS03-015, and MS03-020 this cumulative patch will cause window.showHelp() to cease to function if you have not applied the HTML Help update. If you have installed the updated HTML Help control from Knowledge Base article 811630, you will still be able to use HTML Help functionality after applying this patch.*

After releasing MS03-032, Microsoft identified a problem with the patch. The only affected configurations are Windows XP systems running the web server component of Internet Information Services (IIS) 5.1 with .NET Framework 1.0 serving ASP.NET web pages. Clients using such servers may receive error messages when attempting to view web pages. More information, including a workaround, is available in Microsoft Knowledge Base Article 827641.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS03-040.

Appendix B References

- CERT/CC Vulnerability Note VU#205148 - <http://www.kb.cert.org/vuls/id/205148>
- CERT/CC Vulnerability Note VU#865940 - <http://www.kb.cert.org/vuls/id/865940>
- CERT/CC Vulnerability Note VU#548964 - <http://www.kb.cert.org/vuls/id/548964>
- CERT/CC Vulnerability Note VU#813208 - <http://www.kb.cert.org/vuls/id/813208>
- CERT/CC Vulnerability Note VU#334928 - <http://www.kb.cert.org/vuls/id/334928>
- CERT/CC Vulnerability Note VU#25249 - <http://www.kb.cert.org/vuls/id/25249>
- eEye Digital Security Advisory AD20030820 - <http://www.eeye.com/html/Research/Advisories/AD20030820.html>
- SNS Advisory No. 67 - <http://www.lac.co.jp/security/english/snsadv_e/67_e.html>
- SNS Advisory No. 68 - <http://www.lac.co.jp/security/english/snsadv_e/68_e.html>
- Microsoft Security Bulletin MS03-032 - <http://microsoft.com/technet/security/bulletin/MS03-032.asp>
- Microsoft Security Bulletin MS03-040 - <http://microsoft.com/technet/security/bulletin/MS03-040.asp>
- Microsoft KB Article 822925 - <http://support.microsoft.com/?id=822925>
- Microsoft KB Article 811630 - <http://support.microsoft.com/?id=811630>
- Microsoft KB Article 827641 - <http://support.microsoft.com/?id=827641>
- ASP.NET Fix for 'Server Application Unavailable' Error - <http://www.asp.net/faq/ms03-32-issue.aspx>

Microsoft credits eEye Digital Security, LAC, and KPMG UK for reporting these vulnerabilities. Information from eEye, LAC, and Microsoft was used in this document.

Feedback can be directed to the author, Art Manion.

Revision History

August 26, 2003: Initial release

September 3, 2003: Added patch warning about WinXP/.NET web servers

September 9, 2003: Noted patch does not address VU#865940 and point to workarounds

October 4, 2003: Added information about MS03-040

October 6, 2003: Fixed VU#865490 typo, fixed CAN-2003-808 reference, added #revision tag

23 CA-2003-23: RPCSS Vulnerabilities in Microsoft Windows

Original release date: September 10, 2003
Last revised: September 12, 2003
Source: CERT/CC

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

Systems Affected

- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0, Terminal Server Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Overview

Microsoft has published a bulletin describing three vulnerabilities that affect numerous versions of Microsoft Windows. Two of these vulnerabilities are remotely exploitable buffer overflows that may allow an attacker to execute arbitrary code with system privileges. The third vulnerability may allow a remote attacker to cause a denial of service.

I. Description

The Microsoft RPCSS Service is responsible for managing Remote Procedure Call (RPC) messages. There are two buffer overflow vulnerabilities in the RPCSS service, which is enabled by default on many versions of Microsoft Windows. These buffer overflows occur in sections of code that handle DCOM activation messages sent to the RPCSS service.

The CERT/CC is tracking these vulnerabilities as VU#483492 and VU#254236, which correspond to CVE candidates CAN-2003-0715 and CAN-2003-0528, respectively. The buffer overflows discussed in this advisory are different than those discussed in previous advisories.

Microsoft has also published information regarding a denial-of-service vulnerability in the RPCSS service. This vulnerability only affects Microsoft Windows 2000 systems.

The CERT/CC is tracking this vulnerability as VU#326746, which corresponds to CVE candidate CAN-2003-0605. This vulnerability was previously discussed in CA-2003-19.

According to Microsoft, Windows Millennium Edition (ME) has been tested and is not affected by the vulnerabilities listed in MS03-039.

Important Notice Regarding Scanning Tools

There is an important side effect to applying the patch provided by MS03-039. Specifically, application of this patch will cause many scanning tools to incorrectly report that a system patched by MS03-039 is missing the patch provided in MS03-026.

Microsoft has provided a *new* scanning tool that correctly detects hosts that require either the MS03-026 or MS03-039 patch. To obtain this tool, please read Microsoft Knowledge Base Article 827363.

It is important that all users discontinue the use of scanning tools intended for MS03-026 and obtain an updated tool that detects both MS03-026 and MS03-039. This also applies to sites that use a third-party scanning tool.

II. Impact

By exploiting either of the buffer overflow vulnerabilities, remote attackers may be able to execute arbitrary code with Local System privileges.

By exploiting the denial-of-service vulnerability, remote attackers may be able to disrupt the RPCSS service. This may result in general system instability and require a reboot.

III. Solution

Apply a patch from Microsoft

Microsoft has published Microsoft Security Bulletin MS03-039 to address this vulnerability. For more information, please see http://www.microsoft.com/technet/security/bulletin/MS03-039.asp.

The patches provided in MS03-039 supersede those provided in both MS03-026 and MS01-048.

Block traffic to and from common Microsoft RPC ports

As an interim measure, users can reduce the chance of successful exploitation by blocking traffic to and from well-known Microsoft RPC ports, including

- Port 135 (tcp/udp)
- Port 137 (udp)
- Port 138 (udp)
- Port 139 (tcp)
- Port 445 (tcp/udp)
- Port 593 (tcp)

To prevent compromised hosts from contacting other vulnerable hosts, the CERT/CC recommends that system administrators filter the ports listed above for both incoming and outgoing traffic.

Disable COM Internet Services and RPC over HTTP

COM Internet Services (CIS) is an optional component that allows RPC messages to be tunneled over HTTP ports 80 and 443. As an interim measure, sites that use CIS may wish to disable it as an alternative to blocking traffic to and from ports 80 and 443.

Disable DCOM

Disable DCOM as described in MS03-039 and Microsoft Knowledge Base Article 825750.

This document was written by Jeffrey P. Lanza and is based upon the information in MS03-039.

Revision History

```
Sep 10, 2003: Initial release

Sep 10, 2003: Added links to Vulnerability Notes

Sep 12, 2003: Added scanning tool information to description

Sep 12, 2003: Updated solution section to include reference to MS01-
048

Sep 12, 2003: Added information about Windows ME to description
```

24 CA-2003-24: Buffer Management Vulnerability in OpenSSH

Original release date: September 16, 2003
Last revised: Aug 12, 2008
Source: CERT/CC

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

Systems Affected

- Systems running versions of OpenSSH prior to 3.7.1
- Systems that use or derive code from vulnerable versions of OpenSSH

Overview

There is a remotely exploitable vulnerability in a general buffer management function in versions of OpenSSH prior to 3.7.1. This may allow a remote attacker to corrupt heap memory which could cause a denial-of-service condition. It may also be possible for an attacker to execute arbitrary code.

I. Description

We are updating this advisory to inform users that Version 3.7.1 of OpenSSH has been released to patch a similar vulnerability in the buffer management code.

There are two errors in the buffer management code of OpenSSH. These vulnerabilities affect versions prior to 3.7.1. Version 3.7 is affected by one of these errors. The errors occur when a buffer is allocated for a large packet. When the buffer is cleared, an improperly sized chunk of memory is filled with zeros. This leads to heap corruption, which could cause a denial-of-service condition. These vulnerabilities may also allow an attacker to execute arbitrary code.

The OpenSSH advisory has been updated to include a patch for version 3.7 as well as 3.6.1 and prior.

http://www.openssh.com/txt/buffer.adv

Other systems that use or derive code from OpenSSH may be affected. This includes network equipment and embedded systems. We have monitored incident reports that may be related to this vulnerability.

Vulnerability Note VU#333628 lists the vendors we contacted about these vulnerabilities. The vulnerability note is available from

http://www.kb.cert.org/vuls/id/333628

This vulnerability has been assigned the following Common Vulnerabilities and Exposures (CVE) number:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0693

II. Impact

While the full impact of this issues are unclear, the most likely result is heap corruption, which could lead to a denial of service.

If it is possible for an attacker to execute arbitrary code, then they may be able to so with the privileges of the user running the sshd process, typically root. This impact may be limited on systems using the privilege separation (privsep) feature available in OpenSSH.

III. Solution

Upgrade to OpenSSH version 3.7.1

This vulnerability is resolved in OpenSSH version 3.7.1, which is available from the OpenSSH web site at

http://www.openssh.com/

Apply a patch from your vendor

A patches for these issues are included in the OpenSSH advisory at

http://www.openssh.com/txt/buffer.adv

This patch may be manually applied to correct this vulnerability in affected versions of OpenSSH. If your vendor has provided a patch or upgrade, you may want to apply it rather than using the patch from OpenSSH. Find information about vendor patches in Appendix A. We will update this document as vendors provide additional information.

Use privilege separation to minimize impact

System administrators running OpenSSH versions 3.2 or higher may be able to reduce the impact of this vulnerability by enabling the "UsePrivilegeSeparation" configuration option in their sshd configuration file. Typically, this is accomplished by creating a privsep user, setting up a restricted (chroot) environment, and adding the following line to /etc/ssh/sshd_config:

```
UsePrivilegeSeparation yes
```

This workaround does **not** prevent this vulnerability from being exploited, however due to the privilege separation mechanism, the intruder may be limited to a constrained chroot environment with restricted privileges. This workaround will not prevent this vulnerability from creating a denial-of-service condition. Not all operating system vendors have implemented the privilege separation code, and on some operating systems it may limit the functionality of OpenSSH. System administrators are encouraged to carefully review the implications of using the workaround in their environment and use a more comprehensive solution if one is available. The use of privilege separation to limit the impact of future vulnerabilities is encouraged.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in the revision history. Additional vendors who have not provided direct statements, but who have made public statements or informed us of their status are listed in VU#333628. If a vendor is not listed below or in VU#333628, we have not received their comments.

AppGate Network Security AB

AppGate versions from 4.0 up to and including 5.3.1 does include the vulnerable code. Patches are available from the appgate support pages at http://www.appgate.com.

Apple Computers Inc.

Mac OS X 10.2.8 contains the patches to address CVE CAN-2003-0693, CAN-2003-0695, and CAN-2003-0682. On Mac OS X versions prior to 10.2.8, the vulnerability is limited to a denial of service from the possibility of causing sshd to crash. Each login session has its own sshd, so established connections are preserved up to the point where system resources are exhausted by an attack.

To deliver the update in a rapid and reliable manner, only the patches for CVE IDs listed above were applied, and not the entire set of patches for OpenSSH 3.7.1. Thus, the OpenSSH version in Mac OS X 10.2.8, as obtained via the "ssh -V" command, is:

```
OpenSSH_3.4p1+CAN-2003-0693, SSH protocols 1.5/2.0, OpenSSL 0x0090609f
```

Mac OS X 10.2.8 is available as a free update for customers running Mac OS X 10.2.x. It is available from:

Mac OS X Client (updating from 10.2 - 10.2.5):
http://www.info.apple.com/kbnum/n120244

Mac OS X Client (updating from 10.2.6 - 10.2.7):
http://www.info.apple.com/kbnum/n120245

Mac OS X Server (updating from 10.2 - 10.2.5):
http://www.info.apple.com/kbnum/n120246

Mac OS X Server (updating from 10.2.6 - 10.2.7):
http://www.info.apple.com/kbnum/n120247

Bitvise

Our software shares no codebase with the OpenSSH implementation, therefore we believe that, in our products, this problem does not exist.

Cisco

Cisco has some products which are vulnerable to this issue. Cisco's response is now published at

http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml

Cray, Inc.

Cray Inc. supports OpenSSH through its Cray Open Software (COS) package. Cray is vulnerable to this buffer management error and is in the process of compiling OpenSSH 3.7. The new version will be made available in the next COS release.

Debian

Debian has issued DSA 382 and DSA 383 for these issues.

http://www.debian.org/security/2003/dsa-382
http://www.debian.org/security/2003/dsa-383

F-Secure

This vulnerability does not affect any version of F-Secure SSH software that utilizes ssh protocol version 2. The non-affected versions have been available since 1998.

This vulnerability only affects the following F-Secure SSH server versions: F-Secure SSH for Unix versions 1.3.14 and earlier.

More information is available from

http://www.f-secure.com/support/technical/ssh/ssh1_openssh_buffer_management.shtml

IBM AIX

The AIX Security Team is aware of the issues discussed in CERT
Vulnerability Note VU#333628 and CERT Advisory CA-2003-24.

OpenSSH is available for AIX via the AIX Toolbox for Linux or the
Bonus Pack.

OpenSSH 3.4p1, revision 9 contains fixes for this issue for the AIX Toolbox
for Linux. For more information about the AIX Toolbox for Linux or to download

OpenSSH 3.4p1 revision 9, please see:

http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html

Please note that AIX Toolbox for Linux is available "as-is" and is unwarranted.

Patched versions of OpenSSH for the Bonus Pack on AIX 5.1 and 5.2 are available
Please see:

http://oss.software.ibm.com/developerworks/projects/opensshi

Juniper Networks

Juniper Networks has identified this vulnerability in all shipping versions of JUNOS and coded a software fix. The fix will be included in all releases of JUNOS Internet software built on or after September 17. Customers with current support contracts should contact JTAC to obtain the fix for this vulnerability.

JUNOSe and SDX are not vulnerable to this issue.

Contract customers can review the details at:

https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2003-09-007&actionBtn=Search

Mandrake Software

Mandrake Linux is affected and MDKSA-2003:090 will be released today with patched versions of OpenSSH to resolve this issue.

Mirapoint

Mirapoint released a patch (D3_SSH_CA_2003_24) last night to fix the first reported vulnerability and will release D3_SSH_CA_2003_24_1 to cover the second.

NetBSD

The NetBSD Security Advisory on the OpenSSH buffer management issue is available here:

ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-012.txt.asc

Network Appliance

This issue applies only to SecureAdmin on Data ONTAP versions earlier than 6.4.3, and SecureAdmin for NetCache releases earlier than 5.5R2.

All current releases (NetCache 5.6, 6.0 and 6.1, and Filer 6.5, 7.0, 7.1, 7.2, 7.3 and 10.0) have been secured against this issue.

If you have an affected release:

Disable the SSH server on the filer or NetCache appliance, or if it must remain enabled, ensure that the ssh.access option (config.admin.trusted_hosts in NetCache) is used to restrict ssh connections to authorized administrative hosts.

Openwall GNU/*/Linux

The OpenSSH package in Openwall GNU/*/Linux did contain the buffer / memory management errors. As of 2003/09/17, we have included the fixes from OpenSSH 3.7.1 as well as 4 additional fixes to other such real or potential errors based on an exhaustive review of the OpenSSH source code for uses of *realloc() functions. At this time, it is uncertain whether and which of these bugs are exploitable. If exploits are possible, due to privilege separation, the worst direct impact should be limited to arbitrary code execution under the sshd pseudo-user account restricted within the chroot jail /var/empty, or under the logged in user account

Pragma Systems

We have tested our code and double checked for the code vulnerability and we have found that our code is NOT vulnerable.

PuTTY

PuTTY is not based on the OpenSSH code base, so it should not be vulnerable to any OpenSSH-specific attacks.

Red Hat, Inc.

Red Hat Linux and Red Hat Enterprise Linux ship with an OpenSSL package vulnerable to these issues. Updated OpenSSL packages are available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Linux:

http://rhn.redhat.com/errata/RHSA-2003-279.html

Red Hat Enterprise Linux:

http://rhn.redhat.com/errata/RHSA-2003-280.html

Riverstone Networks

Riverstone Networks has issued an advisory on this issue at http://www.riverstonenet.com/support/tb0265-9.html.

Secure Computing Corporation

Sidewinder(r) and Sidewinder G2 Firewall(tm) (including all appliances)

Not Vulnerable.

Sidewinder v5.x & Sidewinder G2 v6.x's embedded Type Enforcement(r) technology strictly limits the capabilities of Secure Computing's modified version of the OpenSSH daemon code integrated into the firewall's SecureOS operating system. Any attempt to exploit this vulnerability in the OpenSSH daemon code running on the firewalls results in an automatic termination of the attacker's connection and multiple Type Enforcement alarms.

Gauntlet(tm) & e-ppliance

Not Vulnerable.

Gauntlet and e-ppliance do not include SSH server software, and are thus immune to this vulnerability.

SSH Communications Security

SSH Secure Shell products do not contain the buffer management error. SSH Communications Security products have different code base than OpenSSH.

Sun Microsystems

The Solaris Secure Shell in Solaris 9 is impacted by this issue described in CERT Vulnerability Note VU#333628. Sun has published Sun Alert 56861 available here:

http://sunsolve.sun.com/search/document.do?assetkey=1-26-56861-1

which details the impact, contributing factors, workaround options, and resolution. This issue does not affect the Solaris Secure Shell in Solaris 10.

The CERT/CC thanks Markus Friedl of the OpenSSH project for his technical assistance in producing this advisory.

Authors: Jason A. Rafail and Art Manion

Revision History

```
September 16, 2003: Initial release
```

September 17, 2003: Updated with new information regarding 3.7.1 release

September 17, 2003: Added SSH Communications Security vendor statement

September 17, 2003: Added Red Hat, Inc. vendor statement

September 17, 2003: Added Sun Microsystems vendor statement

September 17, 2003: Added NetBSD vendor statement

September 17, 2003: Added Network Appliance vendor statement

September 18, 2003: Added Cisco vendor statement

September 18, 2003: Updated Red Hat, Inc. links in vendor statement

September 18, 2003: Added IBM vendor statement

September 18, 2003: Added F-Secure vendor statement

September 18, 2003: Added OpenWall GNU/*/Linux vendor statement

September 22, 2003: Added Juniper Networks vendor statement

September 22, 2003: Added Mirapoint vendor statement

September 23, 2003: Added Secure Computing Corp. vendor statement

September 23, 2003: Added AppGate Network Security AB vendor statement

October 01, 2003: Added Apple Computers vendor statement

October 01, 2003: Added Pragma Systems vendor statement

October 01, 2003: Updated IBM vendor statement

October 01, 2003: Added Riverstone vendor statement

January 16, 2007: Updated Sun vendor statement

August 12, 2008: Updated Network Appliance vendor statement

25 CA-2003-25: Buffer Overflow in Sendmail

Original issue date: October 1, 2003
Last revised: October 23, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- OpenSSL versions prior to 0.9.7c and 0.9.6k
- Multiple SSL/TLS implementations
- SSLeay library

Overview

There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities may allow a remote attacker to execute arbitrary code. The common impact is denial of service.

I. Description

SSL and TLS are used to provide authentication, encryption, and integrity services to higher-level network applications such as HTTP. Cryptographic elements used by the protocols, such as X.509 certificates, are represented as ASN.1 objects. In order to encode and decode these objects, many SSL and TLS implementations (and cryptographic libraries) include ASN.1 parsers.

OpenSSL is a widely deployed open source implementation of the SSL and TLS protocols. OpenSSL also provides a general-purpose cryptographic library that includes an ASN.1 parser.

The U.K. National Infrastructure Security Co-ordination Centre (NISCC) has developed a test suite to analyze the way SSL and TLS implementations handle exceptional ASN.1 objects contained in client and server certificate messages. Although the test suite focuses on certificate messages, any untrusted ASN.1 element may be used as an attack vector. An advisory from OpenSSL describes as vulnerable "Any application that makes use of OpenSSL's ASN1 library to parse untrusted data. This includes all SSL or TLS applications, those using S/MIME (PKCS#7) or certificate generation routines."

There are two certificate message attack vectors. An attacker can send crafted client certificate messages to a server, or attempt to cause a client to connect to a server under the attacker's control. When the client connects, the attacker can deliver a crafted server certificate message. Note that the standards for TLS (RFC 2246) and SSL 3.0 state that a client certificate message "...is only sent if the server requests a certificate." To reduce exposure to these types of attacks, an SSL/TLS server should ignore unsolicited client certificate messages (VU#732952).

NISCC has published two advisories describing vulnerabilities in OpenSSL (006489/OpenSSL) and other SSL/TLS implementations (006489/TLS). The second advisory covers multiple vulnerabilities in many vendors' products. Further details, including vendor status information, are available in the following vulnerability notes.

VU#935264 - OpenSSL ASN.1 parser insecure memory deallocation
A vulnerability in the way OpenSSL deallocates memory used to store ASN.1 structures could allow a remote attacker to execute arbitrary code with the privileges of the process using the OpenSSL library.

(Other resources: NISCC/006490/OpenSSL/3, OpenSSL #1, CAN-2003-0545)

VU#255484 - OpenSSL contains integer overflow handling ASN.1 tags (1)
An integer overflow vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service.

(Other resources: NISCC/006489/OpenSSL/1, OpenSSL #2, CAN-2003-0543)

VU#380864 - OpenSSL contains integer overflow handling ASN.1 tags (2)
A second integer overflow vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service.

(Other resources: NISCC/006489/OpenSSL/1, OpenSSL #2, CAN-2003-0544)

VU#686224 - OpenSSL does not securely handle invalid public key when configured to ignore errors
A vulnerability in the way OpenSSL handles invalid public keys in client certificate messages could allow a remote attacker to cause a denial of service. This vulnerability requires as a precondition that an application is configured to ignore public key decoding errors, which is not typically the case on production systems.

(Other resources: NISCC/006489/OpenSSL/2, OpenSSL #3)

VU#732952 - OpenSSL accepts unsolicited client certificate messages
OpenSSL accepts unsolicited client certificate messages. This could allow an attacker to exploit underlying flaws in client certificate handling, such as the vulnerabilities listed above.

(Other resources: OpenSSL #4)

VU#104280 - Multiple vulnerabilities in SSL/TLS implementations
Multiple vulnerabilities exist in different vendors' SSL/TLS implementations. The impacts of these vulnerabilities include remote execution of arbitrary code, denial of service, and disclosure of sensitive information. VU#104280 covers an undefined set of vulnerabilities that affect SSL/TLS implementations from many different vendors. The other vulnerabilities listed above are specific to OpenSSL.

(Other resources: NISCC/006489/TLS)

II. Impact

The impacts of these vulnerabilities vary. In almost all, a remote attacker could cause a denial of service. For at least one vulnerability in OpenSSL (VU#935264), a remote attacker may be able to execute arbitrary code. Please see Appendix A, the Systems Affected section of VU#104280, and the OpenSSL vulnerability notes for details.

III. Solution

Upgrade or apply a patch

To resolve the OpenSSL vulnerabilities, upgrade to OpenSSL 0.9.7c or OpenSSL 0.9.6k. Alternatively, upgrade or apply a patch as directed by your vendor. Recompile any applications that are statically linked to OpenSSL libraries.

For solutions for the other SSL/TLS vulnerabilities covered by VU#104280, please see Appendix A and the Systems Affected section of VU#104280.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated, and the changes are noted in the revision history. If a vendor is not listed below, we have not received their authenticated, direct statement. Further vendor information is available in the Systems Affected sections of the vulnerability notes listed above.

AppGate Network Security AB

The default configuration of AppGate is not vulnerable. However some extra functionality which administrators can enable manually may cause the system to become vulnerable. For more details check the AppGate support pages at http://www.appgate.com/support.

Apple Computer Inc.

Apple: Vulnerable. This is fixed in Mac OS X 10.2.8 which is available from http://www.apple.com/support/

Check Point

Check Point products are vulnerable to: VU#732952 09/04/2003 OpenSSL accepts unsolicited client certificate messages VU#380864 09/30/2003 OpenSSL contains integer overflow handling ASN.1 tags (2) VU#255484 09/30/2003 OpenSSL contains integer overflow handling ASN.1 tags (1) A fix will be released by Oct 27th 2003. Check Point products are not vulnerable to: VU#686224 09/30/2003 OpenSSL does not securely handle invalid public key when configured to ignore errors VU#935264 09/30/2003 OpenSSL ASN.1 parser insecure memory deallocation

Clavister

Clavister Firewall: Not vulnerable

As of version 8.3, Clavister Firewall implements an optional HTTP/S server for purposes of user authentication. However, since this implementation does not support client certificates and has no ASN.1 parser code, there can be no ASN.1-related vulnerabilities as far as SSL is concerned.

Earlier versions of Clavister Firewall do not implement any SSL services.

Cray Inc.

Cray Inc. supports OpenSSL through its Cray Open Software (COS) package. The OpenSSL version in COS 3.4 and earlier is vulnerable. Spr 726919 has been opened to address this.

cryptlib

cryptlib does not appear to be vulnerable to the malformed ASN.1 data, either with or without the use of its internal ASN.1 firewall.

Debian

Corrected OpenSSL packages are available in Debian Security Advisory 393, at http://www.debian.org/security/2003/dsa-393 [See also: DSA-394.]

F5 Networks

F5 products BIG-IP, 3-DNS, ISMan and Firepass are vulnerable. F5 will have ready security patches for each of these products. Go to ask.f5.com for the appropriate security response instructions for your product.

Hitachi

Hitachi is investigating the potential impact to Hitachi's software products. As further information becomes available Hitachi will provide notice of the Information.

Hitachi Web Server is under investigation. (Since there was a non-investigated portion, it is under re-investigation.)

IBM

[AIX]

The AIX Security Team is aware of the issues discussed in CERT Vulnerability Notes VU#255484, VU#380864, VU#686224, VU#935264 and VU#732952.

OpenSSL is available for AIX via the AIX Toolbox for Linux. Please note that the Toolbox is made available "as-is" and is unwarranted. The Toolbox ships with OpenSSL 0.9.6g which is vulnerable to the issues referenced above. A patched version of OpenSSL will be provided shortly and this vendor statement will be updated at that time.

Please note that OpenSSH, which is made available through the Expansion Pack is not vulnerable to these issues.

[eServer]

IBM eServer Platform Response

For information related to this and other published CERT Advisories that may relate to the IBM eServer Platforms (xSeries, iSeries, pSeries, and zSeries) please go to https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&pathID=

In order to access this information you will require a Resource Link ID. To subscribe to Resource Link go to http://app-06.www.ibm.com/servers/resourcelink and follow the steps for registration.

All questions should be refered to servsec@us.ibm.com.

Ingrian Networks

Ingrian Networks is aware of this vulnerablity and will issue a security advisory when our investigation is complete.

Juniper Networks

The OpenSSL code included in domestic versions of JUNOS Internet Software that runs on all M-series and T-series routers is susceptible to these vulnerabilities. The SSL library included in Releases 2.x and 3.x of SDX provisioning software for E-series routers is susceptible to these vulnerabilities.

Solution Implementation

Corrections for all the above vulnerabilities are included in all versions of JUNOS built on or after October 2, 2003. Customers should contact Juniper Networks Technical Assistance Center (JTAC) for instructions on obtaining and installing the corrected code.

SDX software built on or after October 2, 2003, contain SSL libraries with corrected code. Contact JTAC for instructions on obtaining and installing the corrected code.

MandrakeSoft

The vulnerabilities referenced by VU#255484, VU#380864, and VU#935264 have been corrected by packages released in our MDKSA-2003:098 advisory.

NEC Corporation

Subject: VU#104280

sent on October 1, 2003

[Server Products]

- EWS/UP 48 Series operating system
  - is NOT vulnerable.
  It doesn't include SSL/TLS implementation.

Nortel Networks

The SSL implementation of the following Nortel Networks products is based on OpenSSL and may be affected by the vulnerabilities identified in NISCC Vulnerability Advisory 006489/OpenSSL:

Alteon Switched Firewall
Alteon iSD - SSL Accelerator
Contivity
Succession Communication Server 2000 - Compact (CS2K - Compact)
Preside Service Provisioning

Other Nortel Networks products with SSL implementations are being reviewed and this Vendor Statement may be revised.

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

Novell is reviewing our application portfolio to identify products affected by the vulnerabilities reported by the NISCC. We have the patched OpenSSL code and are reviewing and testing it internally, and preparing patches for our products that are affected. We expect the first patches to become available via our Security Alerts web site (http://support.novell.com/security-alerts) during the week of 6 Oct 2003. Customers are urged to monitor our web site for patches to versions of our products that they use and apply them expeditiously.

OpenSSL

Please see OpenSSL Security Advisory [30 September 2003].

Openwall GNU/*/Linux

Openwall GNU/*/Linux currently uses OpenSSL 0.9.6 branch and thus was affected by the ASN.1 parsing and client certificate handling vulnerabilities pertaining to those versions of OpenSSL. It was not affected by the potentially more serious incorrect memory deallocation vulnerability (VU#935264, CVE CAN-2003-0545) that is specific to OpenSSL 0.9.7.

Owl-current as of 2003/10/01 has been updated to OpenSSL 0.9.6k, thus correcting the vulnerabilities.

Red Hat

Red Hat distributes OpenSSL 0.9.6 in various Red Hat Linux distributions and with the Stronghold secure web server. Updated packages which contain backported patches for these issues are available along with our advisories at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Enterprise Linux:
http://rhn.redhat.com/errata/RHSA-2003-293.html

Red Hat Linux 7.1, 7.2, 7.3, 8.0:
http://rhn.redhat.com/errata/RHSA-2003-291.html

Stronghold 4 cross-platform:
http://rhn.redhat.com/errata/RHSA-2003-290.html

Red Hat distributes OpenSSL 0.9.7 in Red Hat Linux 9. Updated packages which contain backported patches for these issues are available along with our advisory at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Linux 9:
http://rhn.redhat.com/errata/RHSA-2003-292.html

Riverstone Networks

Riverstone Networks routers are not vulnerable.

RSA Security

The issues raised in this vulnerability report have been analysed in terms of impact on RSA BSAFE SSL-C, RSA BSAFE SSL-C Micro Edition, and RSA BSAFE Cert-C Micro Edition. None of these issues have been determined by RSA Security to be security critical, the products are either not impacted by the vulnerabilities raised or the impact is limited to additional Denial of Sevice opportunities.

As part of RSA Security standard product support lifecycle, fixes for those vulnerabilities which are relevant for each product listed will be incorporated in the next maintenance release. RSA Security customers with current support and maintenance contracts may request a software upgrade for new product versions online at <https://www.rsasecurity.com/go/form_ins.html>.

SCO

We are aware of the issue and are diligently working on a fix. [CSSA-2003-SCO.25]

Secure Computing Corporation

Sidewinder(r) and Sidewinder G2 Firewall(tm) (including all appliances)

Sidewinder v5.x and Sidewinder G2 v6.x are not vulnerable to the arbitrary code execution attacks described in this advisory. The Sidewinder's embedded Type Enforcement technology strictly limits the capabilities of each component which implements SSL. Any attempt to exploit this vulnerability in the SSL library code running on the firewall results in an automatic termination of the attacker's connection and multiple Type Enforcement alarms.

Any component attacked by the denial of service (DOS) attacks described in this advisory is automatically restarted by the firewall's watchdog process without interuption of any active connections. However, under some circumstances this DOS could cause a delay in managing the firewall.

To mitigate this inconvenience, customers should contact Secure Computing Customer Support.

Gauntlet(tm) & e-ppliance

Gauntlet and e-ppliance do not include any components based on OpenSSL, and are thus immune to these vulnerabilities.

SGI

SGI acknowledges receiving the vulnerabilities reported by CERT and NISCC. CAN-2003-0543 [VU#255484], CAN-2003-0544 [VU#380864] and CAN-2003-0545 [VU#935264] have been addressed by SGI Security Advisory 20030904-01-P:

ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc

No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported SGI operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on http://www.sgi.com/support/security/

Sun Microsystems Inc.

Sun is currently investigating Solaris 7, 8, and 9 to determine the full potential impact of these SSL/TLS vulnerabilities.

The Solaris Secure Shell daemon, sshd(1M), shipped with Solaris 9, is not affected by these vulnerabilities.

Java Secure Sockets Extension 1.0.x and J2SE 1.4.x are also not affected.

Sun Linux and Sun Cobalt both ship vulnerable versions of OpenSSL, a Sun Alert has been published here:

http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/57100

Stonesoft

Stonesoft has published a security advisory that addresses the issues in vulnerability notes VU#255484 and VU#104280. The advisory is at http://www.stonesoft.com/document/art/3040.html

Stunnel

Stunnel requires the OpenSSL libraries for compilation (POSIX) or OpenSSL DLLs for runtime operation (Windows). While Stunnel itself is not vulnerable, it's dependence on OpenSSL means that your installation likely is vulnerable.

If you compile from source, you need to install a non-vulnerable version of OpenSSL and recompile Stunnel.

If you use the compiled Windows DLLs from stunnel.org, you should download new versions which are not vulnerable. OpenSSL 0.9.7c DLLs are available at http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7c/

No new version of Stunnel source or executable will be made available, because the problems are inside OpenSSL -- Stunnel itself does not have the vulnerability.

SuSE

All SuSE products are affected. Update packages are being tested and will be published on Wednesday, October 1st. [SuSE-SA:2003:043]

VanDyke

None the VanDyke Software products are subject to these vulnerabilities due to the fact that OpenSSL is not used in any VanDyke products.

Appendix B References

- CERT/CC Vulnerability Note VU#935264 - <http://www.kb.cert.org/vuls/id/935264>
- CERT/CC Vulnerability Note VU#255484 - <http://www.kb.cert.org/vuls/id/255484>
- CERT/CC Vulnerability Note VU#380864 - <http://www.kb.cert.org/vuls/id/380864>
- CERT/CC Vulnerability Note VU#686224 - <http://www.kb.cert.org/vuls/id/686224>

- CERT/CC Vulnerability Note VU#732952 - <http://www.kb.cert.org/vuls/id/732952>
- CERT/CC Vulnerability Note VU#104280 - <http://www.kb.cert.org/vuls/id/104280>
- OpenSSL Security Advisory [30 September 2003] - <http://www.openssl.org/news/secadv_20030930.txt>
- NISCC Vulnerability Advisory 006489/OpenSSL - <http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm>
- NISCC Vulnerability Advisory 006489/TLS - <http://www.uniras.gov.uk/vuls/2003/006489/tls.htm>
- ITU ASN.1 documentation - <http://www.itu.int/ITU-T/studygroups/com10/languages/>

NISCC discovered and researched these vulnerabilities; this document is based on their work. We would like to thank Stephen Henson of the OpenSSL project and the Oulu University Secure Programming Group (OUSPG) for their previous work in this area.

Feedback can be directed to the author, Art Manion.

Revision History

October 1, 2003: Initial release, added RSA Security statement

October 2, 2003: Updated SuSE statement

October 3, 2003: Updated SCO statement

October 8, 2003: Added Debian statement, updated Hitachi statement

October 15, 2003: Added Secure Computing statement

October 22, 2003: Added Check Point and cryptlib statements, updated RSA statement, fixed NISCC references

October 23, 2003: Updated Debian statement

October 24, 2003: Added Sun and Nortel statements

26 CA-2003-26: Multiple Vulnerabilities in SSL/TLS Implementations

Original issue date: October 1, 2003
Last revised: October 23, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- OpenSSL versions prior to 0.9.7c and 0.9.6k
- Multiple SSL/TLS implementations
- SSLeay library

Overview

There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities may allow a remote attacker to execute arbitrary code. The common impact is denial of service.

I. Description

SSL and TLS are used to provide authentication, encryption, and integrity services to higher-level network applications such as HTTP. Cryptographic elements used by the protocols, such as X.509 certificates, are represented as ASN.1 objects. In order to encode and decode these objects, many SSL and TLS implementations (and cryptographic libraries) include ASN.1 parsers.

OpenSSL is a widely deployed open source implementation of the SSL and TLS protocols. OpenSSL also provides a general-purpose cryptographic library that includes an ASN.1 parser.

The U.K. National Infrastructure Security Co-ordination Centre (NISCC) has developed a test suite to analyze the way SSL and TLS implementations handle exceptional ASN.1 objects contained in client and server certificate messages. Although the test suite focuses on certificate messages, any untrusted ASN.1 element may be used as an attack vector. An advisory from OpenSSL describes as vulnerable "Any application that makes use of OpenSSL's ASN1 library to parse untrusted data. This includes all SSL or TLS applications, those using S/MIME (PKCS#7) or certificate generation routines."

There are two certificate message attack vectors. An attacker can send crafted client certificate messages to a server, or attempt to cause a client to connect to a server under the attacker's control. When the client connects, the attacker can deliver a crafted server certificate message. Note that the standards for TLS (RFC 2246) and SSL 3.0 state that a client certificate message "...is only sent if the server requests a certificate." To reduce exposure to these types of attacks, an SSL/TLS server should ignore unsolicited client certificate messages (VU#732952).

NISCC has published two advisories describing vulnerabilities in OpenSSL (006489/OpenSSL) and other SSL/TLS implementations (006489/TLS). The second advisory covers multiple vulnerabilities in many vendors' products. Further details, including vendor status information, are available in the following vulnerability notes.

VU#935264 - OpenSSL ASN.1 parser insecure memory deallocation
A vulnerability in the way OpenSSL deallocates memory used to store ASN.1 structures could allow a remote attacker to execute arbitrary code with the privileges of the process using the OpenSSL library.

(Other resources: NISCC/006490/OpenSSL/3, OpenSSL #1, CAN-2003-0545)

VU#255484 - OpenSSL contains integer overflow handling ASN.1 tags (1)
An integer overflow vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service.

(Other resources: NISCC/006489/OpenSSL/1, OpenSSL #2, CAN-2003-0543)

VU#380864 - OpenSSL contains integer overflow handling ASN.1 tags (2)
A second integer overflow vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service.

(Other resources: NISCC/006489/OpenSSL/1, OpenSSL #2, CAN-2003-0544)

VU#686224 - OpenSSL does not securely handle invalid public key when configured to ignore errors
A vulnerability in the way OpenSSL handles invalid public keys in client certificate messages could allow a remote attacker to cause a denial of service. This vulnerability requires as a precondition that an application is configured to ignore public key decoding errors, which is not typically the case on production systems.

(Other resources: NISCC/006489/OpenSSL/2, OpenSSL #3)

VU#732952 - OpenSSL accepts unsolicited client certificate messages
OpenSSL accepts unsolicited client certificate messages. This could allow an attacker to exploit underlying flaws in client certificate handling, such as the vulnerabilities listed above.

(Other resources: OpenSSL #4)

VU#104280 - Multiple vulnerabilities in SSL/TLS implementations
Multiple vulnerabilities exist in different vendors' SSL/TLS implementations. The impacts of these vulnerabilities include remote execution of arbitrary code, denial of service, and disclosure of sensitive information. VU#104280 covers an undefined set of vulnerabilities that affect SSL/TLS implementations from many different vendors. The other vulnerabilities listed above are specific to OpenSSL.

(Other resources: NISCC/006489/TLS)

II. Impact

The impacts of these vulnerabilities vary. In almost all, a remote attacker could cause a denial of service. For at least one vulnerability in OpenSSL (VU#935264), a remote attacker may be able to execute arbitrary code. Please see Appendix A, the Systems Affected section of VU#104280, and the OpenSSL vulnerability notes for details.

III. Solution

Upgrade or apply a patch

To resolve the OpenSSL vulnerabilities, upgrade to OpenSSL 0.9.7c or OpenSSL 0.9.6k. Alternatively, upgrade or apply a patch as directed by your vendor. Recompile any applications that are statically linked to OpenSSL libraries.

For solutions for the other SSL/TLS vulnerabilities covered by VU#104280, please see Appendix A and the Systems Affected section of VU#104280.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated, and the changes are noted in the revision history. If a vendor is not listed below, we have not received their authenticated, direct statement. Further vendor information is available in the Systems Affected sections of the vulnerability notes listed above.

AppGate Network Security AB

The default configuration of AppGate is not vulnerable. However some extra functionality which administrators can enable manually may cause the system to become vulnerable. For more details check the AppGate support pages at http://www.appgate.com/support.

Apple Computer Inc.

Apple: Vulnerable. This is fixed in Mac OS X 10.2.8 which is available from http://www.apple.com/support/

Check Point

Check Point products are vulnerable to: VU#732952 09/04/2003 OpenSSL accepts unsolicited client certificate messages VU#380864 09/30/2003 OpenSSL contains integer overflow handling ASN.1 tags (2) VU#255484 09/30/2003 OpenSSL contains integer overflow handling ASN.1 tags (1) A fix will be released by Oct 27th 2003. Check Point products are not vulnerable to: VU#686224 09/30/2003 OpenSSL does not securely handle invalid public key when configured to ignore errors VU#935264 09/30/2003 OpenSSL ASN.1 parser insecure memory deallocation

Clavister

Clavister Firewall: Not vulnerable

As of version 8.3, Clavister Firewall implements an optional HTTP/S server for purposes of user authentication. However, since this implementation does not support client certificates and has no ASN.1 parser code, there can be no ASN.1-related vulnerabilities as far as SSL is concerned.

Earlier versions of Clavister Firewall do not implement any SSL services.

Cray Inc.

Cray Inc. supports OpenSSL through its Cray Open Software (COS) package. The OpenSSL version in COS 3.4 and earlier is vulnerable. Spr 726919 has been opened to address this.

cryptlib

cryptlib does not appear to be vulnerable to the malformed ASN.1 data, either with or without the use of its internal ASN.1 firewall.

Debian

Corrected OpenSSL packages are available in Debian Security Advisory 393, at http://www.debian.org/security/2003/dsa-393 [See also: DSA-394.]

F5 Networks

F5 products BIG-IP, 3-DNS, ISMan and Firepass are vulnerable. F5 will have ready security patches for each of these products. Go to ask.f5.com for the appropriate security response instructions for your product.

Hitachi

Hitachi is investigating the potential impact to Hitachi's software products. As further information becomes available Hitachi will provide notice of the Information.

Hitachi Web Server is under investigation. (Since there was a non-investigated portion, it is under re-investigation.)

IBM

[AIX]

The AIX Security Team is aware of the issues discussed in CERT Vulnerability Notes VU#255484, VU#380864, VU#686224, VU#935264 and VU#732952.

OpenSSL is available for AIX via the AIX Toolbox for Linux. Please note that the Toolbox is made available "as-is" and is unwarranted. The Toolbox ships with OpenSSL 0.9.6g which is vulnerable to the issues referenced above. A patched version of OpenSSL will be provided shortly and this vendor statement will be updated at that time.

Please note that OpenSSH, which is made available through the Expansion Pack is not vulnerable to these issues.

[eServer]

IBM eServer Platform Response

For information related to this and other published CERT Advisories that may relate to the IBM eServer Platforms (xSeries, iSeries, pSeries, and zSeries) please go to https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&pathID=

In order to access this information you will require a Resource Link ID. To subscribe to Resource Link go to http://app-06.www.ibm.com/servers/resourcelink and follow the steps for registration.

All questions should be refered to servsec@us.ibm.com.

Ingrian Networks

Ingrian Networks is aware of this vulnerablity and will issue a security advisory when our investigation is complete.

Juniper Networks

The OpenSSL code included in domestic versions of JUNOS Internet Software that runs on all M-series and T-series routers is susceptible to these vulnerabilities. The SSL library included in Releases 2.x and 3.x of SDX provisioning software for E-series routers is susceptible to these vulnerabilities.

Solution Implementation

Corrections for all the above vulnerabilities are included in all versions of JUNOS built on or after October 2, 2003. Customers should contact Juniper Networks Technical Assistance Center (JTAC) for instructions on obtaining and installing the corrected code.

SDX software built on or after October 2, 2003, contain SSL libraries with corrected code. Contact JTAC for instructions on obtaining and installing the corrected code.

MandrakeSoft

The vulnerabilities referenced by VU#255484, VU#380864, and VU#935264 have been corrected by packages released in our MDKSA-2003:098 advisory.

NEC Corporation

Subject: VU#104280

sent on October 1, 2003

[Server Products]

- EWS/UP 48 Series operating system
  - is NOT vulnerable.
  It doesn't include SSL/TLS implementation.

Nortel Networks

The SSL implementation of the following Nortel Networks products is based on OpenSSL and may be affected by the vulnerabilities identified in NISCC Vulnerability Advisory 006489/OpenSSL:

Alteon Switched Firewall
Alteon iSD - SSL Accelerator
Contivity
Succession Communication Server 2000 - Compact (CS2K - Compact)
Preside Service Provisioning

Other Nortel Networks products with SSL implementations are being reviewed and this Vendor Statement may be revised.

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

Novell is reviewing our application portfolio to identify products affected by the vulnerabilities reported by the NISCC. We have the patched OpenSSL code and are reviewing and testing it internally, and preparing patches for our products that are affected. We expect the first patches to become available via our Security Alerts web site (http://support.novell.com/security-alerts) during the week of 6 Oct 2003. Customers are urged to monitor our web site for patches to versions of our products that they use and apply them expeditiously.

OpenSSL

Please see OpenSSL Security Advisory [30 September 2003].

Openwall GNU/*/Linux

Openwall GNU/*/Linux currently uses OpenSSL 0.9.6 branch and thus was affected by the ASN.1 parsing and client certificate handling vulnerabilities pertaining to those versions of OpenSSL. It was not affected by the potentially more serious incorrect memory deallocation vulnerability (VU#935264, CVE CAN-2003-0545) that is specific to OpenSSL 0.9.7.

Owl-current as of 2003/10/01 has been updated to OpenSSL 0.9.6k, thus correcting the vulnerabilities.

Red Hat

Red Hat distributes OpenSSL 0.9.6 in various Red Hat Linux distributions and with the Stronghold secure web server. Updated packages which contain backported patches for these issues are available along with our advisories at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Enterprise Linux:
http://rhn.redhat.com/errata/RHSA-2003-293.html

Red Hat Linux 7.1, 7.2, 7.3, 8.0:
http://rhn.redhat.com/errata/RHSA-2003-291.html

Stronghold 4 cross-platform:
http://rhn.redhat.com/errata/RHSA-2003-290.html

Red Hat distributes OpenSSL 0.9.7 in Red Hat Linux 9. Updated packages which contain back-ported patches for these issues are available along with our advisory at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Linux 9:
http://rhn.redhat.com/errata/RHSA-2003-292.html

Riverstone Networks

Riverstone Networks routers are not vulnerable.

RSA Security

The issues raised in this vulnerability report have been analysed in terms of impact on RSA BSAFE SSL-C, RSA BSAFE SSL-C Micro Edition, and RSA BSAFE Cert-C Micro Edition. None of these issues have been determined by RSA Security to be security critical, the products are either not impacted by the vulnerabilities raised or the impact is limited to additional Denial of Sevice opportunities.

As part of RSA Security standard product support lifecycle, fixes for those vulnerabilities which are relevant for each product listed will be incorporated in the next maintenance release. RSA Security customers with current support and maintenance contracts may request a software upgrade for new product versions online at <https://www.rsasecurity.com/go/form_ins.html>.

SCO

We are aware of the issue and are diligently working on a fix. [CSSA-2003-SCO.25]

Secure Computing Corporation

Sidewinder(r) and Sidewinder G2 Firewall(tm) (including all appliances)

Sidewinder v5.x and Sidewinder G2 v6.x are not vulnerable to the arbitrary code execution attacks described in this advisory. The Sidewinder's embedded Type Enforcement technology strictly limits the capabilities of each component which implements SSL. Any attempt to exploit this vulnerability in the SSL library code running on the firewall results in an automatic termination of the attacker's connection and multiple Type Enforcement alarms.

Any component attacked by the denial of service (DOS) attacks described in this advisory is automatically restarted by the firewall's watchdog process without interuption of any active connections. However, under some circumstances this DOS could cause a delay in managing the firewall.

To mitigate this inconvenience, customers should contact Secure Computing Customer Support.

Gauntlet(tm) & e-ppliance

Gauntlet and e-ppliance do not include any components based on OpenSSL, and are thus immune to these vulnerabilities.

SGI

SGI acknowledges receiving the vulnerabilities reported by CERT and NISCC. CAN-2003-0543 [VU#255484], CAN-2003-0544 [VU#380864] and CAN-2003-0545 [VU#935264] have been addressed by SGI Security Advisory 20030904-01-P:

ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc

No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported SGI operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on http://www.sgi.com/support/security/

Sun Microsystems Inc.

Sun is currently investigating Solaris 7, 8, and 9 to determine the full potential impact of these SSL/TLS vulnerabilities.

The Solaris Secure Shell daemon, sshd(1M), shipped with Solaris 9, is not affected by these vulnerabilities.

Java Secure Sockets Extension 1.0.x and J2SE 1.4.x are also not affected.

Sun Linux and Sun Cobalt both ship vulnerable versions of OpenSSL, a Sun Alert has been published here:

http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/57100

Stonesoft

Stonesoft has published a security advisory that addresses the issues in vulnerability notes VU#255484 and VU#104280. The advisory is at http://www.stonesoft.com/document/art/3040.html

Stunnel

Stunnel requires the OpenSSL libraries for compilation (POSIX) or OpenSSL DLLs for runtime operation (Windows). While Stunnel itself is not vulnerable, it's dependence on OpenSSL means that your installation likely is vulnerable.

If you compile from source, you need to install a non-vulnerable version of OpenSSL and recompile Stunnel.

If you use the compiled Windows DLLs from stunnel.org, you should download new versions which are not vulnerable. OpenSSL 0.9.7c DLLs are available at http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7c/

No new version of Stunnel source or executable will be made available, because the problems are inside OpenSSL -- Stunnel itself does not have the vulnerability.

SuSE

All SuSE products are affected. Update packages are being tested and will be published on Wednesday, October 1st. [SuSE-SA:2003:043]

VanDyke

None the VanDyke Software products are subject to these vulnerabilities due to the fact that OpenSSL is not used in any VanDyke products.

Appendix B References

- CERT/CC Vulnerability Note VU#935264 - <http://www.kb.cert.org/vuls/id/935264>
- CERT/CC Vulnerability Note VU#255484 - <http://www.kb.cert.org/vuls/id/255484>
- CERT/CC Vulnerability Note VU#380864 - <http://www.kb.cert.org/vuls/id/380864>
- CERT/CC Vulnerability Note VU#686224 - <http://www.kb.cert.org/vuls/id/686224>

- CERT/CC Vulnerability Note VU#732952 - <http://www.kb.cert.org/vuls/id/732952>
- CERT/CC Vulnerability Note VU#104280 - <http://www.kb.cert.org/vuls/id/104280>
- OpenSSL Security Advisory [30 September 2003] - <http://www.openssl.org/news/secadv_20030930.txt>
- NISCC Vulnerability Advisory 006489/OpenSSL - <http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm>
- NISCC Vulnerability Advisory 006489/TLS - <http://www.uniras.gov.uk/vuls/2003/006489/tls.htm>
- ITU ASN.1 documentation - <http://www.itu.int/ITU-T/studygroups/com10/languages/>

NISCC discovered and researched these vulnerabilities; this document is based on their work. We would like to thank Stephen Henson of the OpenSSL project and the Oulu University Secure Programming Group (OUSPG) for their previous work in this area.

Feedback can be directed to the author, Art Manion.

Revision History

October 1, 2003: Initial release, added RSA Security statement

October 2, 2003: Updated SuSE statement

October 3, 2003: Updated SCO statement

October 8, 2003: Added Debian statement, updated Hitachi statement

October 15, 2003: Added Secure Computing statement

October 22, 2003: Added Check Point and cryptlib statements, updated RSA statement, fixed NISCC references

October 23, 2003: Updated Debian statement

October 24, 2003: Added Sun and Nortel statements

27 CA-2003-27: Multiple Vulnerabilities in Microsoft Windows and Exchange

Original issue date: October 16, 2003
Last revised: October 17, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Multiple versions of Microsoft Windows (ME, NT 4.0, NT 4.0 TSE, 2000, XP, Server 2003)
- Microsoft Exchange Server 5.5 and Microsoft Exchange Server 2000

Overview

There are multiple vulnerabilities in Microsoft Windows and Microsoft Exchange, the most serious of which could allow remote attackers to execute arbitrary code.

I. Description

There are a number of vulnerabilities in Microsoft Windows and Microsoft Exchange that could allow an attacker to gain administrative control of a vulnerable system. The most serious of these vulnerabilities allow an unauthenticated, remote attacker to execute arbitrary code with no action required on the part of the victim. For detailed information, see the following vulnerability notes:

VU#575892 - Buffer overflow in Microsoft Windows Messenger Service
There is a buffer overflow in the Messenger service on most recent versions of Microsoft Windows that could allow an attacker to execute arbitrary code.

(Other resources: MS03-043, CAN-2003-0717)

VU#422156 - Microsoft Exchange Server fails to properly handle specially crafted SMTP extended verb requests
Microsoft Exchange fails to handle certain SMTP extended verbs correctly. In Exchange 5.5, this can lead to a denial-of-service condition. In Exchange 2000, this could permit an attacker to run arbitrary code.

(Other resources: MS03-046, CAN-2003-0714)

In addition, several other vulnerabilities may permit an attacker to execute arbitrary code if the attacker can convince the victim to take some specific action (e.g., viewing a web page or an HTML email message). For detailed information, see the following vulnerability notes:

VU#467036 - Microsoft Windows Help and Support Center contains buffer overflow in code used to handle HCP protocol
There is a buffer overflow in the Microsoft Windows Help and Support Center that could permit an attacker to execute arbitrary code with SYSTEM privileges.

(Other resources: MS03-044, CAN-2003-0711)

VU#989932 - Microsoft Windows contains buffer overflow in Local Troubleshooter ActiveX control (Tshoot.ocx)
Microsoft Windows ships with a troubleshooting application to assist users with problems. A vulnerability in this application may permit a remote attacker to execute arbitrary code with the privileges of the current user.

(Other resources: MS03-042, CAN-2003-0662)

VU#838572 - Microsoft Windows Authenticode mechanism installs ActiveX controls without prompting user
A vulnerability in Microsoft's Authenticode could allow a remote attacker to install an untrusted ActiveX control on the victim's system. The ActiveX control could run code of the attacker's choice.

(Other resources: MS03-041, CAN-2003-0660)

VU#435444 - Microsoft Outlook Web Access (OWA) contains cross-site scripting vulnerability in the "Compose New Message" form
There is a cross-site scripting vulnerability in Microsoft Outlook Web Access.

(Other resources: MS03-047, CAN-2003-0712)

Finally, there is a vulnerability in ListBox and ComboBox controls that could allow a local user to gain elevated privileges. For detailed information, see

VU#967668 - Microsoft Windows ListBox and ComboBox controls vulnerable to buffer overflow when supplied crafted Windows message
There is a buffer overflow in a function called by the Microsoft Windows ListBox and ComboBox controls that could allow a local attacker to execute arbitrary code with privileges of the process hosting the controls.

(Other resources: MS03-045, CAN-2003-0659)

II. Impact

The impact of these vulnerabilities ranges from denial of service to the ability to execute arbitrary code.

III. Solution

Disable the Messenger Service

For VU#575892, Microsoft recommends first disabling the Messenger service and then evaluating the need to apply the patch. If the Messenger service is not required, leave it in the disabled state. Apply the patch to make sure that systems are protected, especially if the Messenger service is re-enabled. Instructions for disabling the Messenger service can be found in VU#575892 and MS03-043.

Apply patches

Microsoft has provided patches for these problems. Details can be found in the relevant Microsoft Security Bulletins. For many home users, the simplest way to obtain these patches will be by running Windows Update.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated, and the changes are noted in the revision history. If a vendor is not listed below, we have not received their authenticated, direct statement. Further vendor information is available in the Systems Affected sections of the vulnerability notes listed above.

Microsoft Corporation

Please see the following Microsoft Security Bulletins: MS03-041, MS03-042, MS03-043, MS03-044, MS03-045, MS03-046, and MS03-047.

Appendix B References

- CERT/CC Vulnerability Note VU#575892 - http://www.kb.cert.org/vuls/id/575892
- CERT/CC Vulnerability Note VU#422156 - http://www.kb.cert.org/vuls/id/422156
- CERT/CC Vulnerability Note VU#467036 - http://www.kb.cert.org/vuls/id/467036
- CERT/CC Vulnerability Note VU#989932 - http://www.kb.cert.org/vuls/id/989932
- CERT/CC Vulnerability Note VU#838572 - http://www.kb.cert.org/vuls/id/838572
- CERT/CC Vulnerability Note VU#435444 - http://www.kb.cert.org/vuls/id/435444
- CERT/CC Vulnerability Note VU#967668 - http://www.kb.cert.org/vuls/id/967668
- Microsoft Security Bulletin MS03-041 - http://www.microsoft.com/technet/security/bulletin/MS03-041.asp
- Microsoft Security Bulletin MS03-042 - http://www.microsoft.com/technet/security/bulletin/MS03-042.asp
- Microsoft Security Bulletin MS03-043 - http://www.microsoft.com/technet/security/bulletin/MS03-043.asp

- Microsoft Security Bulletin MS03-044 - http://www.microsoft.com/technet/security/bulletin/MS03-044.asp
- Microsoft Security Bulletin MS03-045 - http://www.microsoft.com/technet/security/bulletin/MS03-045.asp
- Microsoft Security Bulletin MS03-046 - http://www.microsoft.com/technet/security/bulletin/MS03-046.asp
- Microsoft Security Bulletin MS03-047 - http://www.microsoft.com/technet/security/bulletin/MS03-047.asp

Our thanks to Microsoft Corporation for the information contained in their security bulletins. Microsoft has credited the following people for their help in discovering and responding to these issues: Greg Jones of KPMG UK and Cesar Cerrudo, The Last Stage of Delirium Research Group, David Litchfield of Next Generation Security Software Ltd., Brett Moore of Security-Assessment.com, Joao Gouveia, and Ory Segal of Sanctum Inc.

Feedback can be directed to the authors, Shawn V. Hernan and Art Manion.

Revision History

October 16, 2003: Initial release, added CAN-2003-0662 reference

October 17, 2003: Fixed MS bulletin references

28 CA-2003-28: Buffer Overflow in Windows Workstation Service

Original release date: November 11, 2003
Last revised: Nov. 20, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows 2000 Service Pack 2, Service Pack 3, Service Pack 4
- Microsoft Windows XP
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition

Overview

A buffer overflow vulnerability exists in Microsoft's Windows Workstation Service (WKSSVC.DLL).

A remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

I. Description

Microsoft's Security Bulletin MS03-049 discusses a buffer overflow in Microsoft's Workstation Service that can be exploited via a specially crafted network message.

According to the eEye Digital Security Advisory AD20031111, the vulnerability is caused by a flaw in the network management functions of the DCE/RPC service and a logging function implemented in Workstation Service (WKSSVC.DLL). Various RPC functions will permit the passing of long strings to the `vsprintf()` routine that is used to create log entries. The `vsprintf()` routine contains no bounds checking for parameters thus creating a buffer overflow situation.

Two exploits and a proof-of-concept exploit have been reported for this vulnerability.

The CERT/CC is tracking this issue as VU#567620. This reference number corresponds to CVE candidate CAN-2003-0812.

II. Impact

A remote attacker could exploit this vulnerability to execute arbitrary code with system-level privileges or to cause a denial of service. The exploit vector and impact for this vulnerability are conducive to automated attacks such as worms.

III. Solution

Apply a patch from your vendor

Apply the appropriate patch as specified in Microsoft Security Bulletin MS03-049.

Appendix A contains additional information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments. Please contact your vendor directly.

Restrict access

You may wish to block access from outside your network perimeter, specifically by blocking access to TCP & UDP ports 138, 139, and 445. This will limit your exposure to attacks. However, blocking at the network perimeter would still allow attackers within the perimeter of your network to exploit the vulnerability. It is important to understand your network's configuration and service requirements before deciding what changes are appropriate.

The CERT/CC has confirmed that one exploit connects to TCP port 445 on the victim machine to exploit this vulnerability. Once exploitation is successful, it then listens on TCP port 4444. You may wish to monitor for this and other open ports as an indication of exploitation.

Disable the Workstation Service

Depending on site requirements, you may wish to disable the Workstation Service as described in MS03-049. Disabling the Workstation Service will help protect against this vulnerability, but may also cause undesirable side effects. According to the Microsoft's Security Bulletin, the impacts of disabling the Workstation Service are as follows:

"If the Workstation service is disabled, the system cannot connect to any shared file resources or shared print resources on a network. Only use this workaround on stand-alone systems (such as many home systems) that do not connect to a network. If the Workstation service is disabled, any services that explicitly depend on the Workstation service do not start, and an error message is logged in the system event log. The following services depend on the Workstation service:

- Alerter
- Browser
- Messenger
- Net Logon

- RPC Locator

These services are required to access resources on a network and to perform domain authentication. Internet connectivity and browsing for stand-alone systems, such as users on dial-up connections, on DSL connections, or on cable modem connections, should not be affected if these services are disabled.

Note: The Microsoft Baseline Security Analyzer will not function if the Workstation service is disabled. It is possible that other applications may also require the Workstation service. If an application requires the Workstation service, simply re-enable the service. This can be performed by changing the Startup Type for the Workstation service back to Automatic and restarting the system."

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments.

Microsoft Corporation

Microsoft has released MS03-049.

This vulnerability was discoved by eEye Digital Security and reported in Microsoft Security Bulletin MS03-049.

Author: Jason A Rafail.

Revision History

```
Nov 11, 2003: Initial release

Nov 20, 2003: Added information regarding exploits
```