Software Engineering Institute
Carnegie Mellon University

1998 CERT Advisories

CERT Division

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

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

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL 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 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.

DM17-0052

Table of Contents

1 CA-1998-01: Smurf IP Denial-of-Service Attacks

Original issue date: January 5, 1998
Last revised: March 13, 2000
Added pointer to RFC2644/BCP34.

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

This advisory is intended primarily for network administrators responsible for router configuration and maintenance.

The attack described in this advisory is different from the denial-of-service attacks described in CERT advisory CA-97.28.

The CERT Coordination Center has received reports from network service providers (NSPs), Internet service providers (ISPs), and other sites of continuing denial-of-service attacks involving forged ICMP echo request packets (commonly known as "ping" packets) sent to IP broadcast addresses. These attacks can result in large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, which can cause network congestion or outages. These attacks have been referred to as "smurf" attacks because the name of one of the exploit programs attackers use to execute this attack is called "smurf."

The CERT/CC urges you to take the steps described in Section III to reduce the potential that your site can be used as the origination site (Sec. III.C) or an intermediary (Sec. III.A.) in this attack. Although there is no easy solution for victim sites, we provide some recommendations in Sec. III.B.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

The two main components to the smurf denial-of-service attack are the use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses.

The Internet Control Message Protocol (ICMP) is used to handle errors and exchange control messages. ICMP can be used to determine if a machine on the Internet is responding. To do this, an ICMP echo request packet is sent to a machine. If a machine receives that packet, that machine will return an ICMP echo reply packet. A common implementation of this process is the "ping" command, which is included with many operating systems and network software packages. ICMP is used to convey status and error information including notification of network congestion and of other network transport problems. ICMP can also be a valuable tool in diagnosing host or network problems.

On IP networks, a packet can be directed to an individual machine or broadcast to an entire network. When a packet is sent to an IP broadcast address from a machine on the local network, that packet is delivered to all machines on that network. When a packet is sent to that IP broadcast address from a machine outside of the local network, it is broadcast to all machines on the target network (as long as routers are configured to pass along that traffic).

IP broadcast addresses are usually network addresses with the host portion of the address having all one bits. For example, the IP broadcast address for the network 10.0.0.0 is 10.255.255.255. If you have subnetted your class A network into 256 subnets, the IP broadcast address for the 10.50 subnet would be 10.50.255.255. Network addresses with all zeros in the host portion, such as 10.50.0.0, can also produce a broadcast response.

In the "smurf" attack, attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. There are three parties in these attacks: the attacker, the intermediary, and the victim (note that the intermediary can also be a victim).

The intermediary receives an ICMP echo request packet directed to the IP broadcast address of their network. If the intermediary does not filter ICMP traffic directed to IP broadcast addresses, many of the machines on the network will receive this ICMP echo request packet and send an ICMP echo reply packet back. When (potentially) all the machines on a network respond to this ICMP echo request, the result can be severe network congestion or outages.

When the attackers create these packets, they do not use the IP address of their own machine as the source address. Instead, they create forged packets that contain the spoofed source address of the attacker's intended victim. The result is that when all the machines at the intermediary's site respond to the ICMP echo requests, they send replies to the victim's machine. The victim is subjected to network congestion that could potentially make the network unusable. Even though we have not labeled the intermediary as a "victim," the intermediary can be victimized by suffering the same types of problem that the "victim" does in these attacks.

Attackers have developed automated tools that enable them to send these attacks to multiple intermediaries at the same time, causing all of the intermediaries to direct their responses to the same victim. Attackers have also developed tools to look for network routers that do not filter broadcast traffic and networks where multiple hosts respond. These networks can the subsequently be used as intermediaries in attacks.

For a more detailed description of the "smurf" attack, please consult this document:

"The Latest in Denial of Service Attacks: 'Smurfing': Description and Information to Minimize Effects"
Author: Craig Huegen <chuegen@quadrunner.com>
URLs: http://www.quadrunner.com/~chuegen/smurf.txt and Smurfing: The Latest DoS Attack

II. Impact

Both the intermediary and victim of this attack may suffer degraded network performance both on their internal networks or on their connection to the Internet. Performance may be degraded to the point that the network cannot be used.

A significant enough stream of traffic can cause serious performance degradation for small and mid-level ISPs that supply service to the intermediaries or victims. Larger ISPs may see backbone degradation and peering saturation.

III. Solution

A. Solutions for the Intermediary

1. Disable IP-directed broadcasts at your router.

   One solution to prevent your site from being used as an intermediary in this attack is to disable IP-directed broadcasts at your router. By disabling these broadcasts, you configure your router to deny IP broadcast traffic onto your network from other networks. In almost all cases, IP-directed broadcast functionality is not needed.

   This network management best practice is described in more detail in the following document authored by Daniel Senie of Amaranth Networks Inc.:

   RFC2644/BCP34: Changing the Default for Directed Broadcasts in Routers

   Appendix A contains details on how to disable IP-directed broadcasts for some router vendors. If your vendor is not listed, contact that vendor for instructions.

   You should disable IP-directed broadcasts on all of your routers. It is not sufficient to disable IP-directed broadcasts only on the router(s) used for your external network connectivity. For example, if you have five routers connecting ten LANs at your site, you should turn off IP-directed broadcasts on all five routers.

2. Configure your operating system to prevent the machine from responding to ICMP packets sent to IP broadcast addresses.

   If an intruder compromises a machine on your network, the intruder may try to launch a smurf attack from your network using you as an intermediary. In this case, the intruder would use the compromised machine to send the ICMP echo request packet to the IP broadcast address of the local network. Since this traffic does not travel through a router to reach the machines on the local network, disabling IP-directed broadcasts on your routers is not sufficient to prevent this attack.

   Some operating systems can be configured to prevent the machine from responding to ICMP packets sent to IP broadcast addresses. Configuring machines so that they do not respond to these packets can prevent your machines from being used as intermediaries in this type of attack.

Appendix A also contains details on how to disable responding to ICMP packets sent to IP broadcast addresses on some operating systems. If your operating system is not listed, contact your vendor for instructions.

B. Solutions for the Victim

Unfortunately, there is no easy solution for victims receiving the potentially large number of ICMP echo reply packets. ICMP echo reply traffic (the traffic from the intermediary) could be blocked at the victim's router; however, that will not necessarily prevent congestion that occurs between the victim's router and the victim's Internet service provider. Victims receiving this traffic may need to consult with their Internet service provider to temporarily block this type of traffic in the ISP's network.

Additionally, victims in this position should contact the intermediaries and inform them of the attack and of the steps described in the previous section.)

Victims can use the "whois" command to obtain contact information for the sites. More information on using whois is available in ftp://ftp.cert.org/pub/whois_how_to.

C. Solution for the Site Where Attacks Originate

We recommend filtering outgoing packets that contain a source address from a different network.

Attacks like the smurf attack rely on the use of forged packets, that is, packets for which the attacker deliberately falsifies the origin address. With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can use filtering to reduce the likelihood of your site's networks being used to initiate forged packets.

As we mentioned in CERT advisory CA-97.28 on Teardrop and Land denial-of-service attacks, the best current method to reduce the number of IP-spoofed packets exiting your network is to install filtering on your routers that requires packets leaving your network to have a source address from your internal network. This type of filter prevents a source IP-spoofing attack from your site by filtering all outgoing packets that contain a source address from a different network.

A detailed description of this type of filtering is available in RFC 2267, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" by Paul Ferguson of Cisco Systems, Inc. and Daniel Senie. We recommend it to both Internet Service Providers and sites that manage their own routers. The document is currently available at ftp://ftp.isi.edu/in-notes/rfc2267.txt.

Note this RFC is no longer considered just informational but has been adopted as a Best Common Practice for network administrators as of February, 2000.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Cray Research - A Silicon Graphics Company

Current versions of Unicos and Unicos/mk do not have the ability to reject ICMP requests send to broadcast addresses. We are tracking this problem through SPR 709733.

Cisco Systems

Cisco recommends the following configuration settings as protection against being used as an intermediary in smurf attacks:

1. Disabling IP directed broadcast for all interfaces on which it is not needed. This must be done on all routers in the network, not just on the border routers. The command "no ip directed-broadcast" should be applied to each interface on which directed broadcasts are to be disabled.

   Very few IP applications actually need to use directed broadcasts, and it's extremely rare for such an application to be in use in a network without the knowledge of the network administrator. Nonetheless, as when any functionality is disabled, you should be alert for possible problems.

   This is the preferred solution for most networks.

2. If your network configuration is simple enough for you to create and maintain a list of all the directed broadcast addresses in your network, and if you have a well-defined perimeter separating your own network from potentially hostile networks, consider using a filter at the perimeter to prevent directed broadcasts from entering the network. For example, if your network number is 172.16.0.0, and you uniformly use a subnet mask of 255.255.255.0, then you might use Cisco access list entries like

   ```
   access-list 101 deny ip 0.0.0.0 255.255.255.255 172.16.0.255
   0.0.255.0

   access-list 101 deny ip 0.0.0.0 255.255.255.255 172.16.0.0
   0.0.255.0
   ```

   Note that this is not a complete access list; it's simply two entries. See the Cisco documentation for more information on configuring access lists. The best place to apply such a filter is usually on the incoming side of each router interface that connects to the potentially hostile network.

   This solution may be administratively infeasible for networks using variable-length subnet masks, or which have complex external connectivity. There is also some possibility that legitimate directed broadcasts may be being sent into your network from the outside, especially if you're working in a research environment.

In addition to these protections against being used as an intermediary in a smurf attack, Cisco recommends that you take steps to prevent users within your own network from launching such attacks. For "stub" networks which do not provide transit connectivity (most corporate and institutional networks, many smaller ISPs), this is usually best done by installing filters at the network perimeter to prevent any packets from leaving your network unless their IP source addresses actually lie within your network's address space. For the example network above, you might place the following entry in the incoming access lists on the interface(s) facing your internal network:

```
access-list 101 permit ip 172.16.0.0 0.0.255.255 0.0.0.0
255.255.255.255
```

```
access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
```

Data General Corporation

DG/UX has an option to enable/disable the forwarding of IP broadcast packets. It is disabled by default. This means that if DG/UX is used along the path, it will not forward the attack packets.

DG/UX B2 with Security Option has a 'netctrl' facility which enables the administrator to disable the response to a broadcast ICMP ping message.

DIGITAL EQUIPMENT CORPORATION

Currently DIGITAL products do not deny individual ICMP service to a host. That, outside the intranet, firewalls should protect from this kind of spoof/attack.

If the problem has to be dealt with inside the firewall and the intranet, then policy should address "malicious acts"and the individuals responsible.

FreeBSD, Inc.

In FreeBSD 2.2.5 and up, the tcp/ip stack does not respond to icmp echo requests destined to broadcast and multicast addresses by default. This behaviour can be changed via the sysctl command via mib net.inet.icmp.bmcastecho.

IBM Corporation

AIX 4

There is a network attribute called "bcastping" that controls whether or not responses to ICMP echo packets to the broadcast address are allowed. A value of zero turns off responses and a value of one turns them on. The default is zero (i.e., by default AIX version 4 is not vulnerable to the described denial-of-service attack).

Use the following command to check the value of the bcastping attribute:

```
$ no -o bcastping
```

Use the following command to turn off responses to ICMP broadcast packets (as root):

```
# no -o bcastping=0
```

AIX 3

The "bcastping" attribute does not exist in version 3.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Livingston Enterprises, Inc.

Livingston Enterprises products don't respond to ICMP packets not sent to their own address, but do forward them. They're currently examining the problem to see what kind of solution they can provide.

The NetBSD Project

Under NetBSD you can disable forwarding of directed broadcast packets with this command, as root:

```
        # sysctl -w net.inet.ip.directed-broadcast=0
```

NetBSD will always respond to broadcast ICMP packets. In the future, NetBSD may allow this to be disabled.

Sun Microsystems

To prevent incoming broadcast packets from entering your network (III. A. 1. in this advisory)

Solaris 2.6, 2.5.1, 2.5, 2.4, and 2.3:

```
Use the command:  ndd -set /dev/ip ip_forward_directed_broadcasts 0
```

SunOS 4.1.3_U1 and 4.1.4:

Do the following:

```
Add ``options DIRECTED_BROADCAST=0'' to system configuration

file and rebuild kernel
```

To prevent systems from responding to broadcast ICMP packets (III. A. 2. in this advisory)

Solaris 2.6, 2.5.1, 2.5, 2.4, and 2.3:

```
Use the command: ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

A corresponding variable for ip_respond_to_echo_broadcast does not exist in SunOS 4.1.x.

The CERT Coordination Center thanks Craig A. Huegen. Much of the content in this advisory has been derived from his document on "smurf" attacks. The CERT Coordination Center also thanks Paul Ferguson and Daniel Senie for providing information on network ingress filtering, and John Bashinski of Cisco for his contributions.

Revision History

```
Mar. 13, 2000 Added pointer to RFC2644/BCP34.

Aug. 24, 1998 Updated vendor information for Data General Corpora-
tion.

Aug. 14, 1998 Updated vendor information for Sun Microsystems.

Apr. 28, 1998 Updated vendor information for Cisco Systems and Sun
Microsystems.

Corrected URL for obtaining RFCs

Apr. 10, 1998 Updated vendor information for Cisco Systems

Feb. 10, 1998 Updates to Appendix A - Vendor Information

Jan. 29, 1998 Updated reference to the filtering document (now an
RFC) in Section III-C.

Jan. 13, 1998 Updated vendor information for NetBSD.

Jan. 7, 1998  Updated or added vendor information for Digital Equip-
ment Corporation and Livingston Enterprises
```

2 CA-1998-02: Vulnerabilities in CDE

Original issue date: January 21, 1998
Last revised: June 18, 1998
Minor editorial changes.

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

The CERT Coordination Center has received reports of several vulnerabilities in some implementations of the Common Desktop Environment (CDE). The root cause of these vulnerabilities is that the dtappgather program does not adequately check all information passed to it by users. As a result, it is possible for a local user to gain unauthorized privileged access or cause a denial of service on the system.

We recommend installing a vendor patch as soon as possible. Until you can do so, we encourage you to disable vulnerable copies of the program. Section III.A. of this advisory contains information on checking for potentially vulnerable copies and disabling them. Section III.B and the appendix contains vendor information.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

There are several vulnerabilities in some implementations of the Common Desktop Environment (CDE). The root cause of these vulnerabilities is that the setuid root program "dtappgather" does not adequately check all information passed to it by users. By exploiting these vulnerabilities, an attacker can gain either unauthorized privileged access or cause a denial of service on the system.

II. Impact

Local users are able to gain write access to arbitrary files. This can be leveraged to gain privileged access.

Local users may also be able to remove files from arbitrary directories, thus causing a denial of service.

III. Solution

We recommend installing a vendor patch as soon as possible and disabling the vulnerable program until you can do so. Instructions for determining whether you have a potentially vulnerable version of this program are given in Section A. Vendor patches are discussed in Section B.

A. How to check for and disable potentially vulnerable versions of dtappgather To find potentially vulnerable versions of dtappgather and to disable those programs, use the following find(1) command or a variant. Consult your local system documentation to determine how to tailor the find(1) program on your system.

You will need to run the find(1) command on each system you maintain because the command examines files on local disks only. Substitute the names of your local file systems for FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var. You should do this as root.

Note that this is one long command, though we have separated it onto three lines using backslashes.

```
find FILE_SYSTEM_NAMES -xdev -type f -user root \
    name 'dtappgather' -perm -04000 -exec ls -l '{}' \; \
    -ok chmod u-s '{}' \;
```

This command will find all files on a system that

- are only in the file systems you name (FILE_SYSTEM_NAMES -xdev)
- are regular files (-type f)
- are owned by root (-user root)
- have the name "dtappgather" (-name 'dtappgather')
- are setuid (-perm -04000)

Once found, those files will

- have their names and details printed (-exec ls -l '{}')
- no longer be setuid root, but only if you type `y' in response to the prompt (-ok chmod u-s '{}' \;)

Until you are able to install the appropriate patch, we recommend that you remove the setuid bit from the dtappgather program. Note that doing this will affect the functionality of the dtappgather program for some users. For example, newly created users that have not logged into the CDE desktop may not have any icons in the Application Manager window; existing users may not notice any change in functionality.

B. Obtain and install a patch for this problem. If your vendor has a patch for this problem, we encourage you to apply the patch as soon as possible.

Appendix A contains a list of vendors who have provided information about this problem. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Digital Equipment Corporation

At the time of writing this document, patches(binary kits) are in progress. Distribution of the fix for this problem is expected to begin soon. Digital will provide notice of the completion/availability of the patches through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

Hewlett-Packard Company

This problem is addressed HP Security Bulletin 075. This bulletin can be found at one of these URLs:

(for US, Canada, Asia-Pacific, & Latin-America): http://us-support.external.hp.com

(for Europe): http://europe-support.external.hp.com

Security Bulletin 075: Security Vulnerability in CDE on HP-UX

```
    PLATFORM: HP9000 Series 700/800s running CDE on:

            HP-UX 10.10, HP-UX 10.20,

            HP-UX 10.24 (VVOS),

            HP-UX 11.00

    SOLUTION:  Apply one of:

             PHSS_13723  HP-UX 10.10

             PHSS_13724  HP-UX 10.20

             PHSS_13725  HP-UX 10.30

             PHSS_13772  HP-UX 10.24

             PHSS_13406  HP-UX 11.00
```

IBM Corporation

The version of dtappgather shipped with AIX is vulnerable. The following fixes are in progress:

```
    AIX 3.2:  not vulnerable; CDE not shipped in 3.2

    AIX 4.1:  IX73436
```

AIX 4.2:	IX73437
AIX 4.3:	IX73438

To Order:

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/ or send e-mail toaixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

The Open Group

The Open Group is investigating this vulnerability, and if reproduced will develop a solution and provide a patch for its CDE licensees.

Siemens-Nixdorf Informationssysteme AG

Siemens-Nixdorf provides the TED desktop by TriTeal Corporation as CDE product. TED contains the vulnerable program "dtappgather". We informed TriTeal about this.

Please note: First level support for the TED desktop is done by Siemens-Nixdorf Informationssysteme.

Silicon Graphics, Inc.

Silicon Graphics provides only the third party TriTeal CDE product.

Triteal Corporation provides all support on the SGI offered CDE product. Customers requiring support on the SGI CDE product should contact TriTeal Corporation at 1-800-874-8325, or email support@triteal.com.

For other Silicon Graphics related security information, please see the SGI Security Headquarters website located at: http://www.sgi.com/Support/security/security.html.

Sun Microsystems, Inc.

Sun has released the following patches:

Patch	CDE version
105837-01	1.2
105838-01	1.2_x86
104498-02	1.02

104500-02	1.02_x86
104497-02	1.01
104499-02	1.01_x86

The above patches are available at: http://sunsolve.sun.com/sunsolve/pubpatches.html

Revision History

June 18, 1998 Minor editorial changes.

Feb. 12, 1998 Added information for Siemens-Nixdorf Informationssysteme AG.

Jan. 29, 1998 Updated vendor information for Sun.

3 CA-1998-03: Vulnerability in ssh-agent

Original issue date: January 22, 1998
Last revised: March 2, 1998
Updates section - described two cases in which the vulnerability is present.

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

The text of this advisory was originally released on January 20, 1998, as SNI-23, developed by Secure Networks, Inc. (SNI). To more widely broadcast this information, we are reprinting the SNI advisory here with their permission. Some technical details in the original advisory are not included in this reprint, and these are indicated thus:

{DETAILS NOT INCLUDED}

We have also removed SNI's PGP public key block and added our contact information.

The original advisory is available from
ftp://ftp.secnet.com/pub/advisories/SNI-23.SSH-AGENT.advisory.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

This advisory details a vulnerabily in the SSH cryptographic login program. The vulnerability enables users to use RSA credentials belonging to other users who use the ssh-agent program. This vulnerability may allow an attacker on the same local host to login to a remote server as the user utilizing SSH.

Problem Description:

In order to avoid forcing users of RSA based authentication to go through the trouble of retyping their pass phrase every time they wish to use ssh, slogin, or scp, the SSH package includes a program called ssh-agent, which manages RSA keys for the SSH program. The ssh-agent program creates a mode 700 directory in /tmp, and then creates an AF_UNIX socket in that directory. Later, the user runs the ssh-add program, which adds his private key to the set of keys managed by the ssh-agent program. When the user wishes to access a service which permits him to log in using only his RSA key, the SSH client connects to the AF_UNIX socket, and asks the ssh-agent program for the key.

Unfortunately, when connecting to the AF_UNIX socket, the SSH client is running as super-user, and performs insufficient permissions checking. This makes it possible for users to trick their SSH clients into using credentials belonging to other users. The end result is that any user who utilizes RSA authentication AND uses ssh-agent, is vulnerable. Attackers can utilize this vulnerability to access remote accounts belonging to the ssh-agent user.

{ DETAILS NOT INCLUDED }

Vulnerable Systems:

This vulnerability effects the Unix versions of SSH ONLY.

SSH for unix versions 1.2.17 through 1.2.21 are vulnerable if installed with default permissions. Versions of SSH prior to 1.2.17 are subject to a similar (but different) attack.

F-Secure SSH for Unix systems prior to release 1.3.3 ARE vulnerable.

You can determine the version of SSH you are running by issuing the case sensitive command:

```
% ssh -V
```

Version 1.1 of the windows-based SSH client sold by Data Fellows Inc. under the F-Secure brand name is NOT vulnerable to this attack.

Versions 1.0 and 1.0a of Mac SSH are NOT vulnerable to this attack.

Fix Resolution:

Non-commercial users:

If using the free non-commercial SSH distribution for Unix, administrators are urged to upgrade to SSH 1.2.22 or later. Updated versions of the free unix SSH can be found at ftp://ftp.cs.hut.fi/pub/ssh

Commercial users:

F-Secure SSH version 1.3.3 fixes this security problem. If you are using the commercial Data Fellows SSH package and you have a support contract, you can obtain SSH version 1.3.3 from your local retailer.

Users without a support contract can obtain a diff file which fixes this problem. This file can be obtained from: http://www.DataFellows.com/f-secure/support/ssh/bug/su132patch.html

Workaround:

As a temporary workaround, administrators may remove the setuid bit from the SSH binary. This will prevent the attack from working, but will disable a form of authentication documented as rhosts-RSA. For example, if your SSH binary is in the /usr/local/bin directory, the following command will remove the setuid bit from the SSH binary:

```
# chmod u-s /usr/local/bin/ssh
```

Additional Information

SSH is a cryptographic rsh, rlogin, and rcp replacement. SSH was written by Tatu Ylonen ylo@cs.hut.fi. For more information about the noncommercial unix version of SSH, please see http://www.cs.hut.fi/ssh

Commercial versions of ssh are marketed by Data Fellows Inc. For information about the F-secure ssh derivatives sold by Data Fellows Inc, please see http://www.DataFellows.com/f-secure.

This vulnerability was discovered by David Sacerdote davids@secnet.com.

{ DETAILS NOT INCLUDED }

Copyright Notice

The contents of this advisory are Copyright (C) 1997 Secure Networks Inc, and may be distributed freely provided that no fee is charged for distribution, and that proper credit is given.

You can find Secure Networks papers at ftp://ftp.secnet.com/pub/papers and advisories at ftp://ftp.secnet.com/advisories.

You can browse our web site at http://www.secnet.com.

You can subscribe to our security advisory mailing list by sending mail to majordomo@secnet.com with the line "subscribe sni-advisories".

The CERT Coordination Center thanks Secure Networks, Inc. for permission to reproduce technical content from their advisory SNI-23, which is copyrighted 1997 Secure Networks, Inc.

Revision History

```
Mar 02, 1998  Updates section -  described two cases in which the

vulnerability is present.
```

4 CA-1998-04: Microsoft Windows-based Web Servers access via long file names

Original issue date: February 6, 1998
Last revised: December 9, 1998
Added vendor information for Netscape and O'Reilly & Associates, Inc.

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

An exploitation involving long file names on Microsoft Windows-based web servers has recently been described on public mailing lists. When files on the web server have names longer than 8.3 (8 characters plus a 3-character extension), users can gain unauthorized access to files protected solely by the web server.

The CERT/CC team recommends installing patches from your vendor (see Section III.A and the appendix). Until you are able to do so, we urge you to use the workaround described in Section III.B.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

All 32-bit Microsoft Windows operating systems (commonly known as Win32) can associate two different file names with a stored file, a short name and a long name. The short version, known as 8.3-compliant, is restricted to a length of 8 characters and an extension of 3 characters. This version is required for backward compatibility with DOS. The long version of the file name is not restricted to the 8.3-compliant format but is restricted to a total length of 255 characters.

When Win32 stores a file with a short name (i.e., 8.3-compliant), it associates only that short file name with the file. However, when Win32 stores a file with a long name (i.e., greater than 8 characters), it associates two versions of the file name with the file--the original, long file name and an 8.3-compliant short file name that is derived from the long name in a predictable manner.

Example:

The 8.3-compliant short file name "Abcdefgh.xyz" is represented

1. as is: "Abcdefgh.xyz".

However, the long file name "Abcdefghijk.xyz" is represented:

1. as is: "Abcdefghijk.xyz" and
2. as 8.3-compliant: "Abcdef~1.xyz".

Some Win32-based web servers have not compensated for the two file name versions when restricting access to files that have long names. The web servers attempt to restrict access by building an internal list of restricted file names. However, for files with long names, only the long, and not the short, file name is added to this internal list. This leaves the file unprotected by the web server because the file is still accessible via the short file name.

For example, "Abcdefgh.xyz" (short) would be protected by the web server, but "Abcdefghijk.xyz" (long) would not be completely protected by the web server.

II. Impact

Users are able to gain unauthorized access to files protected solely by the web server.

III. Solution

CERT/CC urges you to immediately apply vendor patches if they are available. Until you are able to do so, we urge you to use the workaround described in Section B below.

A. Obtain and install a patch for this problem.

   Appendix A contains input from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

B. Until you are able to install the appropriate patch, we recommend the following workaround.

   1. Use only 8.3-compliant short file names for the files that you want to have protected solely by the web server. On FAT file systems (16-bit) this can be enforced by enabling (setting to 1) the "Win31FileSystem" registry key (registry path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\).

   2. On NTFS (32-bit), you can disable the creation of the 8.3-compliant short file name for files with long file names by enabling (setting to 1) the "NtfsDisable8dot3NameCreation" registry key (registry path: HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control\FileSystem\). However, this step may cause compatibility problems with 16-bit applications.

   3. Use NTFS-based ACLs (directory or file level access control lists) to augment or replace web server-based security.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Apache

None of the beta releases of Apache for Win32 are vulnerable to this particular problem.

Microsoft

Microsoft IIS 4.0 and PWS 4.0 with the appropriate patch are not vulnerable.

IIS 4.0 and PWS 4.0 maintain certain configuration information about directories and files in a database called the metabase. The metabase does not contain file permissions, but rather Web server-specific information such as requiring SSL encryption, proxy cache setting, and PICS ratings. Actual file and directory permissions are enforced by NTFS and are not affected by this problem.

Earlier version of IIS and PWS are not vulnerable to this issue.

Microsoft has made available a market bulletin for this issue that is available on "Advisories and Solutions" section of the Microsoft Security Advisor web site, http://www.microsoft.com/security. Please consult this bulletin for information on obtaining the patch.

National Center for Supercomputing Applications (NCSA)

The NCSA HTTPd web server does not run on Windows NT. Note that HTTPd is now an unsupported software product of the National Center for Supercomputing Applications.

Netscape

Netscape has provided the following updated information addressing the vulnerability described in this advisory.

```
Enterprise Server 3.51 - This server is not vulnerable to this attack.
```

```
Enterprise Server 3.0 - A patch has been created to fix the problem.
It can be found off of help.netscape.com.
```

```
FastTrack Server 2.01 - A patch has been created to fix the problem.
```

```
FastTrack Server 3.01 - A patch has been created to fix the problem.
```

O'Reilly & Associates, Inc.

O'Reilly WebSite Professional V1 and V2 and WebSite Standard V1.0e+ are not vulnerable to this problem.

The CERT Coordination Center thanks David LeBlanc for his workaround suggestion.

Revision History

```
Dec.  9, 1998  Added vendor information for Netscape and O'Reilly &
Associates, Inc.

Feb. 11, 1998  Advisory name change, updates to Solution Section
III.B, added Acknowledgment.
```

5 CA-1998-05: Multiple Vulnerabilities in BIND

Original issue date: April 8, 1998
Last revised: November 16, 1998
Added vendor information for Data General

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

1. Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Releases
2. Denial-of-Service Vulnerabilities in BIND 4.9 and BIND 8 Releases
3. Denial-of-Service Vulnerability in BIND 8 Releases

I. Description

This advisory describes three distinct problems in BIND. Topic 1 describes a vulnerability that may allow a remote intruder to gain root access on your name server or to disrupt normal operation of your name server. Topics 2 and 3 deal with vulnerabilities that can allow an intruder to disrupt your name server. Detailed descriptions of each problem and its solutions are included in the individual sections on each topic.

II. Impact

Topic 1: A remote intruder can gain root-level access to your name server.

Topics 2 and 3: A remote intruder is able to disrupt normal operation of your name server.

III. Solution

All three problems can be fixed by upgrading to the latest version of BIND, which may be available from your vendor (see Appendix A of this advisory). Questions about the availability of patches from your vendor should be directed to your vendor.

Additionally, the Internet Software Consortium has announced new publicly available versions of BIND on the BIND WWW page (http://www.isc.org/bind.html) and on the USENET newsgroup comp.protocols.dns.bind.

Additionally, patches are provided for Topics 1 and 3, along with steps to take until you can apply the patch or upgrade to the latest version of BIND.

Topic 1: Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Releases

1.A. Description

BIND 4.9 releases prior to BIND 4.9.7 and BIND 8 releases prior to 8.1.2 do not properly bounds check a memory copy when responding to an inverse query request. An improperly or maliciously formatted inverse query on a TCP stream can crash the server or allow an attacker to gain root privileges.

1.B. Determining if your system is vulnerable

The inverse query feature is disabled by default, so only the systems that have been explicitly configured to allow it are vulnerable.

BIND 8

Look at the "options" block in the configuration file (typically /etc/named.conf). If there is a "fake-iquery yes;" line, then the server is vulnerable.

BIND 4.9

Look at the "options" lines in the configuration file (typically /etc/named.boot). If there is a line containing "fake-iquery", then the server is vulnerable.

In addition, unlike BIND 8, inverse query support can be enabled when the server is compiled. Examine conf/options.h in the source. If the line #defining INVQ is not commented out, then the server is vulnerable.

1.C. What To Do

To address this problem, you can disable inverse queries, upgrade to BIND 8.1.2 now that it is available, or apply the patch (see below for more information on the patch). We urge you to disable inverse queries until you can take one of the other steps.

Disabling inverse queries

BIND 8

Disable inverse queries by editing named.conf so that either there is no "fake-iquery" entry in the "options" block or the entry is "fake-iquery no;"

BIND 4.9

Disable inverse queries by editing named.boot, removing any "fake-iquery" entries on "options" lines. Look at conf/options.h in the source. If INVQ has been defined, comment it out and then rebuild and reinstall the server.

Note: Disabling inverse query support can break ancient versions of nslookup. If nslookup fails, replace it with a version from any BIND 4.9 or BIND 8 distribution.

Fixing the Inverse Query Code

BIND 8

Upgrade to BIND 8.1.2 now that it is available (http://www.isc.org/new-bind.html) or apply the patch at this URL: http://www.cert.org/advisories/CA-1998-05/BIND8_patch.txt .

This file is not PGP signed. It has the following MD5 checksum:

```
MD5 (BIND8_patch.txt) = 12fc9d395ff987b1aad17a882ccd7840
```

BIND 4.9

Upgrade to BIND 4.9.7 now that it is available (http://www.isc.org/new-bind.html) or apply the patch at this URL: http://www.cert.org/advisories/CA-1998-05/BIND4.9_patch.txt .

This file is not PGP signed. It has the following MD5 checksum:

```
MD5 (BIND4.9_patch.txt) = 32da0db1c27e4d484e6fcb7901267c2f
```

Notes:

1. We are asking sites to retrieve the patches via FTP rather than including them in the advisory since our experience is that some mail handling systems translate tabs into spaces. This prevents the patch(1) program from working properly.
2. We have not PGP signed the files since our experience is that some implementations of PGP during the extraction process will strip spaces from some lines containing whitespace only. This may prevent the patch(1) program from working

Topic 2: Denial-of-Service Vulnerabilities in BIND 4.9 and BIND 8 Releases

2.A. Description

BIND 4.9 releases prior to BIND 4.9.7 and BIND 8 releases prior to 8.1.2 do not properly bounds check many memory references in the server and the resolver. An improperly or maliciously formatted DNS message can cause the server to read from invalid memory locations, yielding garbage record data or crashing the server. Many DNS utilities that process DNS messages (e.g., dig, nslookup) also fail to do proper bounds checking.

2.B. Determining if your system is vulnerable

Any system running BIND 4.9 prior to 4.9.7 or BIND 8 prior to 8.1.2 is vulnerable.

2.C. What To Do

There are no workarounds for these problems.

BIND 8

Upgrade to BIND 8.1.2 now that it is available.

BIND 4.9

Upgrade to BIND 4.9.7 now that it is available.

Topic 3: Denial-of-Service Vulnerability in BIND 8 Releases

3.A. Description

Assume that the following self-referential resource record is in the cache on a name server:

```
        foo.example.    IN      A       CNAME   foo.example.
```

The actual domain name used does not matter; the important thing is that the target of the CNAME is the same name. The record could be in the cache either because the server was authoritative for it or because the server is recursive and someone asked for it. Once this record is in the cache, issuing a zone transfer request using its name (e.g., "dig @my_nameserver foo.example. axfr") will cause the server to abort().

Most sites will not contain such a record in their configuration files. However, it is possible for an attacker to engineer such a record into the cache of a vulnerable nameserver and thus cause a denial of service.

3.B. Determining if your system is vulnerable

If the BIND 8 server is not recursive and does not fetch glue, then the problem can be exploited only if the self-referential resource record is in a zone for which the server is authoritative.

If the global zone transfer ACL in the options block has been set to deny access and has no self-referential CNAMEs in its authoritative zones, then the server is not vulnerable.

Otherwise, the server is vulnerable. The nameserver is recursive by default, fetches glue by default, and the default global transfer ACL allows all hosts; so many BIND 8 servers will be vulnerable to this problem.

(Note: the in.named(8) man page mentions that sending a SIGINT to the in.named process will dump the current data base and cache to, by default, /var/tmp/named_dump.db. Some sites may find this useful in looking for self-referential CNAMEs. Please see the in.named(8) man page for further details.)

3.C. What To Do

To address this problem, you can apply the workaround described below, upgrade to BIND 8.1.2, or apply the patch provided at the end of this section. Until you can upgrade or apply the patch, we urge you to use the workaround.

Workaround

First set the global zone transfer ACL to deny access to all hosts by adding the following line to the "options" block:

```
            allow-transfer { none; };
```

Next, explicitly authorize zone transfers for each authoritative zone. For example, if the server was authoritative for "example", adding

```
            allow-transfer { any; };
```

to the "zone" statement for "example" would allow anyone to transfer "example".

None of the domains for which the server is authoritative should have self-referential CNAMEs.

Fixing the Problem

Upgrade to BIND 8.1.2, now that it is available, or apply the patch available from the following URL to the BIND 8.1.1 source: http://www.cert.org/advisories/CA-1998-05/BIND8.1.1_patch.txt .

This file is not PGP signed. It has the following MD5 checksum:

```
      MD5 (BIND8.1.1_patch.txt) = 33f9dc2eaf221dd48553f490259c2a8b
```

Notes:

1. We are asking sites to retrieve the patches via FTP rather than including them in the advisory since our experience is that some mail handling systems translate tabs into spaces. This prevents the patch(1) program from working properly.
2. We have not PGP signed the files since our experience is that some implementations of PGP during the extraction process will strip spaces from some lines containing whitespace only. This may prevent the patch(1) program from working properly.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

1. BSD/OS 3.0/3.1 AS SHIPPED is not vulnerable. Sites wishing to enable fake-iquery can install mod M310-025, available at http://www.bsdi.com
2. BSDI will issue a 3.1 mod when a fix is available.
3. BSD/OS is not vulnerable, since we ship bind 4.9.

Caldera Corporation

Workaround for Topic 1:
Disable inverse queries by editing named.conf so that either there is no "fake-iquery" entry in the "options" block, or so that the entry is "fake-iquery no;"

Workaround for Topic 2:
A workaround is to set the global zone transfer ACL to deny access to all hosts by adding the following line to the "options" block allow-transfer { none; }; Next, explicitly authorize zone transfers for each authoritative zone.

For example, if the server was authoritative for "example", adding allow-transfer { any; }; to the "zone" statement for "example" would allow anyone to transfer "example".

None of the domains the server is authoritative for should have self-referential CNAMEs.

Correction for both Topics:
The proper solution is to Upgrade to the bind-8.1.1-5 packages. They can be found on Caldera's FTP site at: ftp://ftp.caldera.com/pub/OpenLinux/updates/1.2/006/RPMS.

The corresponding source code can be found at:ftp://ftp.caldera.com/pub/OpenLinux/updates/1.2/006/SRPMS.

The MD5 checksums (from the "md5sum" command) for these packages are:

- b63ace6eab6eee5cf0608c8a245b5e27 bind-8.1.1-5.i386.rpm
- 4123b0167f5d5769a87cd2d9542a74b4 bind-doc-8.1.1-5.i386.rpm
- e1d506cbcc87d7c1de915d94d03281b1 bind-utils-8.1.1-5.i386.rpm
- eec24c0f816244c4729281867fcebbab bind-8.1.1-5.src.rpm

Upgrade with the following commands:

- rpm -q bind && rpm -U bind-8.1.1-5.i386.rpm
- rpm -q bind-utils && rpm -U bind-utils-8.1.1-5.i386.rpm
- rpm -q bind-doc && rpm -U bind-doc-8.1.1-5.i386.rpm

This and other Caldera security resources are located at:
http://www.caldera.com/tech-ref/security/.

Data General

This problem is fixed in revision R4.20MU04 of DG/UX. The following patches are available for earlier revisions:

Revision	Patch Number
R4.20MU01	tcpip_R4.20MU01.p10
R4.20MU02	tcpip_R4.20MU02.p09
R4.20MU03	tcpip_R4.20MU03.p01
R4.11MU05	tcpip_R4.11MU05.p09
R4.12MU03	tcpip_R4.12MU03.p02

Digital Equipment Corporation

Digital is investigating this problem.

FreeBSD, Inc.

We ship with INVQ not defined. This makes us resistent against the first vulnerability. This is true for all release after 2.2.0 (2.1.* releases are vulnerable but should be upgraded anyway). As we do not yet ship BIND 8, we are also not vulnerable to the 3rd vulnerability.

We advise everyone to upgrade to BIND 4.9.7.

Hewlett-Packard Company

See Hewlett-Packard Security Bulletin "Security Vulnerability in BIND on HP-UX", HPSBUX9808-083, dated August 19, 1998, for details concerning the availability of patches.

Hewlett Packard's HP-UX patches/Security Bulletins/Security patches are available via email and/or WWW (via the browser of your choice) on HP's Electronic Support Center (ESC).

To subscribe to automatically receive future NEW HP Security Bulletins from the HP ESC Digest service via electronic mail, do the following:

From your Web browser, access the URL:
http://us-support.external.hp.com (US,Canada,Asia-Pacific, and Latin-America) or
http://europe-support.external.hp.com (Europe)

Login with your user ID and password (or register for one). Remember to save the User ID assigned to you, and your password.

Once you are in the Main Menu:

To -subscribe- to future HP Security Bulletins, click on "Support Information Digests".

To -review- bulletins already released from the main Menu, click on the "Technical Knowledge Database (Security Bulletins only)".

Near the bottom of the next page, click on "Browse the HP Security Bulletin Archive".

Once in the archive there is another link to our current Security Patch Matrix. Updated daily, this matrix is categorizes security patches by platform/OS release, and by bulletin topic.

To report new security vulnerabilities, send email to security-alert@hp.com.

Please encrypt any exploit information using the security-alert PGP key, available from your local key server, or by sending a message with a -subject- (not body) of 'get key' (no quotes) to security-alert@hp.com.

IBM Corporation

The version of bind shipped with AIX is vulnerable and the following APARs will be available soon:

```
    AIX 4.1.x: IX76958  (fix for Topic 1 only)

    AIX 4.2.x: IX76959  (fix for Topic 1 only)

    AIX 4.3.x: IX76960  (fix for Topic 1 and 3 only)

    AIX 4.3.x: IX76962  (fix for Topic 1, 2, and 3.  This is bind
8.1.2.)
```

Until the official fixes are available, a temporary patch can be found at:
ftp://aix.software.ibm.com/aix/efixes/security.

```
    File                sum               md5

====================================================================

    named.415.tar.Z     64980   157
0e795380b84bf29385d2d946d10406cb

    named.421.tar.Z     44963   157
15a9a006abf4a9d0a0d3210f16d619e5

    named4.430.tar.Z    48236   115
8377b14f74e207707154a9677906f20a

    named8.430.tar.Z    51175   160
e2db14b7055a7424078456bfbfd9bf2d
```

Detached PGP signatures are also available with a ".asc" extension.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Internet Software Consortium

The Internet Software Consortium has announced BIND version 8.1.2 and BIND version 4.9.7.

If you are running BIND 8.1.1 or 8.1 you want to upgrade to 8.1.2. If you are still running BIND-4 rather than BIND-8, you need the security patches contained in 4.9.7. But, you should really just run BIND-8.

The security fixes included in these releases fix a stack overrun that could occur if inverse query support was enabled, and a number of denial of service attacks where malformed packets could cause the server to crash.

Links to the kits are available at: http://www.isc.org/new-bind.html.

NEC Corporation

Topic1 - Some systems are vulnerable. Patches will be available soon, especially for UX/4800 R11.x and R13.x.

Topic2 - Some systems are vulnerable. Patches will be available soon after the release of bind-4.9.7, especially for UX/4800 R11.x and R13.x.

Topic3 - We do not ship BIND 8 with our products so we are not vulnerable to this problem.

Patches will be available from ftp://ftp.meshnet.or.jp/pub/48pub/security.

The NetBSD Project

The first problem can be fixed in NetBSD 1.3, 1.3.1, and -current prior to 19980408 with the supplied BIND 4.9.6 patch. A patch will be made available for the second problem shortly (alternatively, upgrading to BIND 4.9.7 or 8.1.2 when available will also solve this problem.) NetBSD is not affected by the third problem.

Red Hat Software, Inc.

Red Hat fixes will be available at:

Red Hat 5.0

i386:
rpm -Uvh ftp://ftp.redhat.com/updates/5.0/i386/bind-4.9.6-7.i386.rpm

alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/5.0/alpha/bind-4.9.6-7.alpha.rpm

Red Hat 4.2

i386:
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/i386/bind-4.9.6-1.1.i386.rpm

alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/alpha/bind-4.9.6-1.1.alpha.rpm

SPARC:
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/sparc/bind-4.9.6-1.1.sparc.rpm

The Santa Cruz Operation, Inc.

The following SCO products are vulnerable:

- SCO Open Desktop/Open Server 3.0, SCO UNIX 3.2v4
- SCO OpenServer 5.0 (also SCO Internet FastStart)
- SCO UnixWare 2.1
- SCO UnixWare 7

SCO CMW+ 3.0 is not vulnerable as BIND/named is not supported on CMW+ platforms.

Binary versions of BIND 4.9.7 will be available shortly from the SCO ftp site:

cover letter - ftp://ftp.sco.com/SSE/sse012.ltr
replacement binaries - ftp://ftp.sco.com/SSE/sse012.tar.Z

The fix includes binaries for the following SCO operating systems:

- SCO Open Desktop/Open Server 3.0, SCO UNIX 3.2v4
- SCO OpenServer 5.0
- SCO UnixWare 2.1
- SCO UnixWare 7

For the latest security bulletins and patches for SCO products, please refer to http://www.sco.com/security/ .

Silicon Graphics, Inc.

Silicon Graphics Inc. issued Security Advisory, " IRIX BIND DNS Vulnerabilities," 19980603-02-PX, August 6, 1998.

Patches are available via anonymous FTP and your service/support provider.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at: http://www.sgi.com/Support/security.

Sun Microsystems, Inc.

Topic 1: Patches will be produced for Solaris 5.3, 5.4, 5.5, 5.5.1 and 5.6.

Topic 2: Patches will be produced for Solaris 5.3, 5.4, 5.5, 5.5.1 and 5.6.

Topic 3: Bug fix will be integrated in the upcoming release of Solaris.

The CERT Coordination Center thanks Bob Halley and Paul Vixie of Vixie Enterprises, who provided most of the text of this advisory.

Reminder

The Internet Software Consortium will announce new publicly available versions of BIND on the BIND WWW page (http://www.isc.org/bind.html) and on the USENET newsgroup comp.protocols.dns.

Revision History

```
Nov. 16, 1998  Added vendor information for Data General.

Aug. 21, 1998  Updated vendor informaton for HP and SGI.

June 19, 1998  Updated vendor informaton for SGI.

June 18, 1998  Added a pointer to more information in the UPDATES
section.

May 21, 1998   Updates were made to the following portions of this
advisory:

III. Solutions

Topic 1: Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Re-
leases

1.C. What To Do
```

```
Fixing the Inverse Query Code, Bind 8 and Bind 4.9

Topic 2: Denial-of-Service Vulnerabilities in BIND 4.9 and BIND 8
Releases

2.C. What To Do

Topic 3: Denial-of-Service Vulnerability in BIND 8 Releases

3.C. What To Do

Fixing the Problem

Appendix A - Updated vendor information for Internet Software Con-
sortium

Apr. 16, 1998  Appendix A - Updated vendor information for Caldera
Corporation.
```

6 CA-1998-06: Buffer Overflow in NIS+

Original issue date: June 9, 1998
Last revised: Nov 9, 1999
Updated vendor information for Data General.

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

The CERT Coordination Center has received a report from Internet Security Systems regarding a vulnerability in some implementations of NIS+. The NIS+ service is offered by the rpc.nisd program on many systems.

We recommend installing a vendor patch as soon as possible. Until you are able to do that, we encourage you to implement applicable workarounds as described in section III.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

NIS+ and NIS are designed to assist in the administration of networks by providing centralized management and distribution of information about users, machines, and other resources on the network. NIS+ is a replacement for NIS. A buffer overflow exists in some versions of NIS+. At this time, we do not believe any versions of NIS are vulnerable to this buffer overflow. Note that this vulnerability exists independently of the security level at which the NIS+ server is running.

II. Impact

Depending on the configuration of the target machine, a remote intruder can gain root access to a vulnerable system or cause the NIS+ server to crash, which will affect the usability of any system which depends on NIS+.

Additionally, if your NIS+ server is running in NIS compatibility mode and if an intruder is able to crash the NIS+ server, the intruder may be able to masquerade as an NIS server and gain access to machines that depend on NIS for authentication.

Finally, if an intruder is able to crash an NIS+ server and there are clients on the local network that are initialized by broadcast, an intruder may be able to provide false initialization information to the NIS+ clients. Clients that are initialized by hostname may also be vulnerable under some circumstances.

III. Solution

A. Obtain and install a patch from your vendor.

Appendix A contains input from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

B. Until you are able to install the appropriate patch, we recommend the following workaround.
   1. As with any software, particularly network services, if you do not depend on NIS+, we encourage you to disable it.

C. If you must operate with an unpatched version of NIS+, the risk may be mitigated using the following strategies.
   1. Limit external access to your portmapper by blocking access to port 111 at your firewall or router. Additionally, if you have not already done so, apply the patches referenced in VB-97.03, available at ftp://ftp.cert.org/pub/cert_bulletins/VB-97.03.sun.

      Note that restricting access to the portmapper does not necessarily prevent an intruder from connecting directly to the port on which NIS+ is running. For this and other reasons we recommend that any port that is not explicitly required be blocked at your router or firewall.

   2. Configure your system to mark the stack as non-executable. For example, on Solaris systems running on sun4m, sun4d and sun4u platforms, the variable noexec_user_stack in the /etc/system file can be used to mark the stack as non-executable by default. While this will prevent an intruder from gaining root access, it will not prevent an intruder from crashing the NIS+ server. For more information on the noexec_user_stack variable, see http://docs.sun.com:80/ab2/coll.47.4/SYSADMIN1/@Ab2PageView/91907?DwebQuery=executable+stacks.

      Marking the stack as non-executable is highly dependent on hardware and software configurations. For information on marking the stack as non-executable on other platforms, consult your vendor or operating systems manuals.

   3. Initialize newly installed NIS+ clients using a method that does not rely on unauthenticated network information. For example, on Solaris systems you can copy the /var/nis/NIS_COLD_START file from an already existing NIS+ client, and use that file as input to the nisinit command.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Data General

Data General is not vulnerable to this problem.

Digital Equipment Corporation

This problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

FreeBSD, Inc.

```
FreeBSD is not vulnerable.
```

Fujitsu

UXP/V V10L20, the current version of the UNIX-based operating system running on the Fujitsu VPP Series supercomputers, is vulnerable. Fujitsu is currently working on a patch for UXP/V V10L20.

UXP/V V10L10, the version that preceded V10L20, is not vulnerable.

Hewlett-Packard Company

HP-UX is Vulnerable. Patches in process.

IBM Corporation

AIX is not vulnerable.

NEC Corporation

Some NEC systems are vulnerable. Patches are in progress and will be available from ftp://ftp.meshnet.or.jp/pub/48pub/security.

The NetBSD Project

NetBSD is not vulnerable.

OpenBSD

OpenBSD is not vulnerable.

The Santa Cruz Operation, Inc.

No SCO products are vulnerable.

Sun Microsystems, Inc.

Patches were released for Solaris 5.4, 5.5, 5.5.1, and 5.6.

The patch numbers are as follows.

5.4	sparc	101973-35
5.4	intel	101974-35
5.5	sparc	103187-38
5.5	intel	103188-38
5.5.1	sparc	103612-41
5.5.1	intel	103613-41
5.6	sparc	105401-12
5.6	intel	105402-12

Sun estimates that a patch for SunOS 5.3 will be available in about 12

weeks. The expected patch number is 101318-91.

We wish to thank Josh Daymont of ISS who reported the vulnerability and provided technical assistance.

Revision History

```
July 22, 1999  Added vendor information for Fujitsu.


Nov 9, 1999  Updated vendor information for Data General.
```

7 CA-1998-07: Vulnerability in Some Usages of PKCS#1

Original issue date: June 26, 1998
Last revised: August 24, 1998
Added vendor information for Silicon Graphics, Inc.

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

The CERT Coordination Center has received a report regarding a vulnerability in some implementations of products utilizing RSA Laboratories' Public-Key Cryptography Standard #1 (PKCS#1). Under some situations, a sophisticated intruder may be able to use the vulnerability in PKCS#1 to recover information from SSL-encrypted sessions.

The CERT/CC team recommends that sites install patches immediately as described in Appendix A. Appendix A also contains pointers to web pages containing additional information maintained by some vendors.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

PKCS#1 is a standard for encrypting data using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes.

One use for the digital envelopes constructed using PKCS#1 is to provide confidentiality during the session key negotiation of an SSL-encrypted session. The SSL protocol is widely used to encrypt traffic to and from web servers to protect the privacy of information such as personal data or a credit card number, as it traverses the internet. A sophisticated intruder may be able to use the vulnerability in PKCS#1 to recover information from an SSL-encrypted session.

Web pages employing SSL are accessed using the HTTPS protocol, rather than the HTTP protocol.

More information about PKCS#1 can be found at http://www.rsa.com/rsalabs/pubs/PKCS/.

Additional information regarding this vulnerability will be available at http://www.bell-labs.com.

This vulnerability does not affect all PKCS#1-enabled products. The attack is not effective against protocols in which there is not an interactive session setup, or where the error messages returned by the server do not distinguish among the types of failures. In particular, this vulnerability does not affect S/MIME or SET.

II. Impact

Under some circumstances, an intruder who is able to observe an SSL-encrypted session, and subsequently interrogate the server involved in the session, may be able to recover the session key used in that session, and then recover the encrypted data from that session.

The vulnerability can only be exploited if the intruder is able to make repeated session-establishment attempts to the same vulnerable web server which was involved in the original session. In addition, the server must return error messages that distinguish between several modes of failure. Although the number of session-establishment requests is large, it is significantly more efficient than a brute-force attack against the session key. Note that, although web servers comprise the majority of vulnerable servers, other PKCS#1-enabled servers may be vulnerable.

Note that the server's public and private key are not at risk from this vulnerability, and that an intruder is only able to recover data from a single session per attack. Compromising a single session does not give an intruder any additional ability to compromise subsequent sessions. Further, as mentioned above, this vulnerability does not affect all PKCS#1-enabled products.

III. Solution

A. Obtain and install a patch for this problem. Appendix A contains input from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

B. Although applying vendor patches is the recommended course of action, you may wish to consider some of the following steps to reduce your exposure to this vulnerability:

1. Examine your log files for repeated error messages indicating failed requests for session-establishment. For example, sites using C2Net's Stronghold server would see error messages of the form

   ```
   Tue Jun 23 22:08:17 1998] SSL accept error
   1575:error:0407006B:rsa routines:RSA_padding_check_PKCS1_type_2:block type is not
   02:rsa_pk1.c:207
   1575:error:04064072:rsa routines:RSA_EAY_PRIVATE_DECRYPT:padding check
   failed:rsa_eay.c:330
   1575:error:1408B076:SSL routines:SSL3_GET_CLIENT_KEY_EXCHANGE:bad rsa
   decrypt:s3_srvr.c:1259
   ```

   If you are unable to upgrade for an extended period of time, you may wish to consider obtaining a new public/private key pair for servers. Changing the key pair only protects those sessions which may have been previously recorded by an intruder. This does not prevent an intruder from launching attacks against newly-recorded sessions. This should only be considered in those cases where upgrading is infeasible. Again, note that the public/private key pair is not at risk from this vulnerability.
2. Avoid using the same public/private key pair across multiple servers.

3. A large increase in CPU utilization or network traffic may accompany an attack. If your web server does not provide sufficient detail in its logs to detect failures, you may wish to

look for substantial deviation from established usage patterns, which may be indicative of an attack.

Implementors and researchers should consult RSA Laboratories Bulletin Number 7 for additional measures to reduce the effectiveness of this attack. This document will be available at http://www.rsa.com/rsalabs/.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

C2Net Software, Inc.

C2Net has developed a patch and is deploying new builds to combat this problem. More information is available at http://www.c2.net

Microsoft Corporation

The Microsoft Product Security Response Team has produced an update for the following affected Microsoft Internet server software:

- Microsoft Internet Information Server 3.0 and 4.0
- Microsoft Site Server 3.0, Commerce Edition
- Microsoft Site Server, Enterprise Edition
- Microsoft Exchange 5.0 and 5.5 (for SSL-enabled POP3 and SMTP)

Microsoft's Internet server software provides SSL 2.0, SSL 3.0, PCT 1.0, and TLS 1.0 for securing Internet-based communications. These protocols are all implemented in a single file called SCHANNEL.DLL, which is shared by the Microsoft Internet server software listed above. Updating this single file will resolve this vulnerability for these Microsoft server products.

No updates are required for Internet client software, such as Internet Explorer.

This update is now available. Microsoft strongly recommends that customers using secure SSL Internet services with any of the Microsoft products listed above should update to the latest version of SCHANNEL.DLL.

Please visit the Microsoft Security Advisor web site for more information, or link directly to our Microsoft security bulletin MS98-002 at http://www.microsoft.com/security/bulletins/ms98-002.htm.

Netscape Communications Corporation

Netscape recommends that all customers running Netscape Enterprise Server software, Netscape Proxy Server, Netscape Messaging Server and Netscape Collabra Server download and install a simple patch before an attack ever happens.

Product updates and full information about the countermeasures are available immediately from the Netscape Internet site at: http://help.netscape.com/products/server/ssldiscovery/index.html.

Open Market, Inc.

Some of Open Market's products are affected by this vulnerability. Patches are available. For more information, go to http://www.openmarket.com/security.

RSA Data Security, Inc.

Information from RSA regarding this vulnerability is available at http://www.rsa.com/rsalabs/.

Silicon Graphics, Inc.

See Silicon Graphics Inc. Security Advisory, "Vulnerability in Public-Key Cryptography Standard #1 (PKCS#1)," 19980606-01-A, issued June 26, 1998.

Currently, Silicon Graphics Inc. is investigating and is in communication with Netscape. No further information is available for public release at this time.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:
http://www.sgi.com/Support/security.

SSLeay

Information and SSLeay source patches related to this vulnerability are available at http://www.ssleay.org/announce/.

Terisa Systems, Inc. / Spyrus, Inc.

Terisa has determined that the SSL implementation in the Terisa SecureWeb Toolkit is vulnerable to this attack. A patch to fix this vulnerability has been developed for existing versions of the Toolkit. Further information may be found at http://www.terisa.com/.

This vulnerability was originally discovered by Daniel Bleichenbacher of the Secure Systems Research Department of Bell Labs, the research and development arm of Lucent Technologies.

The CERT Coordination Center thanks Scott Schnell of RSA and Jason Garms of Microsoft for reporting this problem to us and providing technical advice and other valuable input into the construction of this advisory. In addition, our thanks goes to Simona Nass, Douglas Barnes, and Tim Hudson of C2Net and David Wagner of the University of California at Berkeley for the example log files contained herein as well as additional technical advice and clarification during the production of this advisory.

Revision History

```
Aug. 24, 1998  Added vendor information for Silicon Graphics, Inc.
```

```
July 27, 1998  Added vendor information for Terisa Systems, Inc. /
Spyrus, Inc.
```

8 CA-1998-08: Buffer Overflows in Some POP Servers

Original issue date: July 14, 1998
Last revised: August 24, 1998
Added vendor information for Silicon Graphics Inc.

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

The CERT Coordination Center has received reports of buffer overflows in some Post Office Protocol (POP) servers. For a list of vulnerable versions and platforms, please refer to Appendix A. For help in determining which version you are currently running, see Section III.A below.

The CERT/CC team recommends that anyone running a vulnerable version of this software upgrade to the current vendor-recommended version. Until you can do so, we suggest disabling the POP server.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

The CERT Coordination Center has received reports of buffer overflow vulnerabilities in some POP servers based on QUALCOMM's qpopper. Qpopper is a Post Office Protocol (POP) server used for downloading Internet e-mail.

Information about this vulnerability has been posted to various mailing lists and newsgroups, and the CERT Coordination Center has received reports of incidents in which this vulnerability has been exploited to gain privileged access.

II. Impact

Remote users can gain privileged (root) access to systems running vulnerable versions of POP servers.

III. Solution

If you determine that your POP server is vulnerable (Sec. A), install a patch from your vendor. Until you can do so, we urge you to disable the POP server.

A. Determine if your version of the POP server is vulnerable.

To determine if a system is vulnerable, first telnet to port 110 on that host. If it is running a POP server, the banner will show the version. For example:

```
% telnet yourmailhost.your.domain.com 110

Trying 123.123.123.123
```

```
                  Connected to mailhost

                  +OK QPOP (version 2.4) at yourmailhost.your.do-
   main.com starting
```

In the above example, the POP server is QUALCOMM's QPopper, version 2.4, which is known to be a vulnerable version.

Check Appendix A to see if your vendor has identified other POP server versions that are vulnerable. If you do not see your vendor's name, please contact the vendor directly.

B. Install a patch for this problem.

Appendix A contains input from vendors who have provided information for this advisory.

C. Workaround

If you are unable to upgrade to a version that is not vulnerable, we urge you to disable the POP server until you are able to address the problem. (This will, of course, mean that the functionality provided by the POP server will not be available.)

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Data General

Data General does not ship qpopper, or any other POP client or server.

Digital Equipment Corporation

Copyright 1994, 1995, 1996, 1997 Compaq Computer Corporation. All rights reserved.

```
SOURCE: Compaq Computer Corporation

        Compaq's Digital UNIX / ULTRIX

        Software Security Response Team USA
```

This reported problem is not present for the as shipped, Compaq's Digital ULTRIX or Compaq's Digital UNIX Operating Systems Software.

Fujitsu

Fujitsu's UXP/V operating system does not support qpopper so we are not affected by it.

OpenBSD

OpenBSD does not ship qpopper.

QUALCOMM Incorporated

Versions of QUALCOMM qpopper prior to 2.5 are vulnerable.

QUALCOMM recommends upgrading to the most recent version (currently Version 2.52). Patches are available from ftp://ftp.qualcomm.com/Eudora/servers/unix/popper.

Further details, questions and comments should be sent to qpopper@qualcomm.com.

Santa Cruz Operation, Inc.

The following releases of SCO Operating Systems contain a version of the Qualcomm popper that is vulnerable:

- SCO OpenServer Releases 5.0.0, 5.0.2, 5.0.4
- SCO Internet FastStart Releases 1.0, 1.1

The following SCO Operating Systems are not vulnerable,

- SCO UnixWare 7
- SCO UnixWare 2.1
- SCO CMW+
- SCO Open Desktop / Open Server 3.0, SCO UNIX 3.2v4

Binary versions of the patched popper will be available shortly from the SCO ftp site:

- ftp://ftp.sco.com/SSE/sse013.ltr - cover letter
- ftp://ftp.sco.com/SSE/sse013.tar.Z - replacement binary

The fix includes binaries for the following SCO operating systems:

- SCO OpenServer 5.0.0, 5.0.2, 5.0.4
- SCO Internet FastStart Releases 1.0, 1.1

For the latest security bulletins and patches for SCO products, please refer to http://www.sco.com/security/.

Silicon Graphics Inc.

Please refer to Silicon Graphics Inc. Security Advisory, "BSD/Qualcomm qpopper Vulnerability," Number: 19980801-01-I, distributed August 6, 1998 for additional information relating to this vulnerability.

The primary SGI anonymous FTP site for security information and patches is sgigate.sgi.com (204.94.209.1). Security information and patches are located under the directories ~ftp/security and ~ftp/patches, respectively. The Silicon Graphics Security Headquarters Web page is accessible at the URL http://www.sgi.com/Support/security/security.html.

The CERT Coordination Center thanks Travis Mikalson at TerraNovaNet, Inc., for reporting the vulnerability, and Laurence Lundblade at QUALCOMM Incorporated for providing technical details and support in the development of the advisory. We also acknowledge other members of the Internet community who posted about this problem.

Revision History

```
Aug. 24, 1998  Added vendor information for Silicon Graphics Inc.

July 22, 1998  Updated vendor information for Fujitsu and Santa

Cruz Operation, Inc.

July 14, 1998  Added vendor information for Digital Equipment Corpo-
ration.
```

9 CA-1998-09: Buffer Overflow in Some Implementations of IMAP Servers

Original issue date: July 20, 1998
Last revised: March 08, 1999
Updated IMAP Server information for ISOCOR.

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

The CERT Coordination Center has received reports regarding a vulnerability in some implementations of IMAP servers.

The CERT/CC recommends that anyone running a vulnerable version of this software upgrade to the current vendor-recommended version. Until you can do so, we suggest disabling the vulnerable IMAP server.

We will update this advisory as we receive additional information. We encourage you to check our web site regularly for updates to this advisory that may relate to your site.

I. Description

The CERT Coordination Center has received reports regarding a buffer overflow in some implementations of IMAP servers. The overflow is in library code from the University of Washington IMAP server that handles SASL server-level authentication. This vulnerability is different from the one discussed in CERT Advisory CA-97.09.imap_pop. Information about this vulnerability has been posted to various public mailing lists and newsgroups.

All versions of the University of Washington IMAP server prior to the final (frozen, non-beta) version of imap-4.1 that support SASL server-level authentication are vulnerable. The vulnerability affects all University of Washington IMAP4rev1 servers prior to v10.234. Also, any v10.234 server that was distributed with Pine 4.0 or any imap-4.1.BETA is vulnerable.

Additionally, the vulnerability is present in other IMAP servers that use library code from the University of Washington IMAP server to handle SASL server-level authentication.

IMAP servers that share no code with the University of Washington server are not vulnerable.

Some operating systems ship with a vulnerable version of this software installed and enabled by default. Please refer to the Vendor Information section below for more information about your vendor.

II. Impact

Remote intruders can execute arbitrary commands under the privleges of the process running the vulnerable IMAP server. If the vulnerable IMAP server is running as root, remote intruders can gain root access.

III. Solution

A. Determine if your version of imapd is vulnerable

To determine if a system is vulnerable, first telnet to port 143 on that host. If it is running an IMAP server, the banner will show the version. For example:

```
% telnet host.your.domain.com 143

Trying 123.123.123.123...

Connected to host.

Escape character is '^]'.

* OK host.your.domain.com IMAP4rev1 v10.190 server ready
```

In the above example, the IMAP server is the University of Washington IMAP4rev1 v10.190. Since all University of Washington IMAP4rev1 servers prior to v10.234 are vulnerable, the server in the above example is vulnerable.

B. Please consult the Vendor Information section below for information about other vulnerable IMAP servers.

C. Install the most recent version of imapd

Obtain and install the most recent version, or patch for your IMAP server. Appendix A contains input from vendors who have provided information for this advisory.

D. Workaround

If you are unable to upgrade to a version that is not vulnerable, we urge you to disable the IMAP server until you are able to address the problem.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

IMAP Server Vendors

Cyrus

This does not affect the Cyrus imapd. Cyrus imapd shares no code with the University of Washington imapd.

Esys Corporation

We are not affected by the problem described in the advisory. We do not ship any University of Washington based software at this time. We have never shipped any of the IMAP 4.x software from the University of Washington.

ISOCOR

No ISOCOR products are affected by this problem. The N-PLEX implementation shares no code with the University of Washington imapd.

Microsoft Corporation

```
No Microsoft products are affected by this problem.
```

NEC Corporation

The University of Washington imapd is shipped with our product "Mobilenet/IMAP" and so it is vulnerable.

Netscape

Netscape Messaging Server 3.55 and before are susceptible to this vulnerability. However, it should be noted that Netscape Messaging Server (any version) does NOT run as root and therefore, the exposure is much more limited than the University of Washington example. Regardless, we have released a patch available at http://help.netscape.com/products/server/messaging which addresses this vulnerability.

Sun Microsystems

Please refer to Sun Microsystems, Inc. Security Bulletin, "IMAP", Number: 00177, distributed October 2, 1998 for additional information relating to this vulnerability.

Patches and Checksums are available to all Sun customers via World Wide Web at:
http://sunsolve.sun.com/sunsolve/pubpatches/patches.html.

Sun security bulletins are available via World Wide Web at:
http://sunsolve.sun.com/sunsolve/secbulletins.

University of Washington

A security problem has been detected with the University of Washington IMAP server that is included in the Pine 4.00 distribution. This will be fixed in the forthcoming Pine 4.01 maintenance release. Until then, if you are using the UW IMAP server, please update it with the following distribution: ftp://ftp.cac.washington.edu/mail/imap.tar.Z.

This vulnerability affects all IMAP4rev1 servers prior to v10.234. v10.234 may or may not be vulnerable; if it came from Pine 4.00 or from any imap-4.1.BETA then it is vulnerable. IMAP2bis servers are immune. This problem is also fixed in the imap-4.2 toolkit, which is tentatively expected to be released in conjunction with Pine 4.01. Any IMAP4rev1 server whose version starts with "v11" will be immune.

Operating System Vendors

Berkeley Software Design, Inc.

The version of IMAP shipped with BSD/OS 2.1 and 3.0/3.1 is the older version which does not include the vulnerability. The version of IMAP which will be included in the upcoming 4.0 release has been updated to include the security fixes.

Caldera Linux

Caldera: releasing patched imap-4.1; will release imap-4.2 as soon as it becomes available.

URL: ftp://ftp.caldera.com/pub/OpenLinux/updates/1.2/010

6df741b4217f03bf773b54509a7d283a imap-4.1.BETA-5.i386.rpm

d3526121c68b611524fc72746204d752 imap-4.1.BETA-5.src.rpm

Compaq Computer Corporation

(c) Copyright 1994, 1995, 1996, 1997, 1998 Compaq Computer Corporation. All rights reserved.

SOURCE: Compaq Computer Corporation

Compaq Services

Software Security Response Team USA

This reported problem is not present for the as shipped,Compaq's Digital ULTRIX or Compaq's Digital UNIX Operating Systems Software.

- Compaq Computer Corporation

Data General

We are investigating. We will provide an update when our investigation is complete.

FreeBSD

FreeBSD does not ship default with imap. However, there is a version of imapd from Washington University in the FreeBSD ports collections, known as imap-uw.

If anyone is using the imap port, we suggest fetching the latest revision of imap and manually install it, or wait until the FreeBSD port is updated and reinstall imap-uw using the ports system You can check the ports status at: http://www.freebsd.org/ports/mail.html.

Fujitsu

Our operating system, UXP/V, does not support imapd. Therefore, it is not vulnerable to the above vulnerability.

Hewlett-Packard Company

HP does not ship the University of Washington IMAP server.

IBM Corporation

The version of imapd shipped with AIX 4.2 and 4.3 is vulnerable. We are currently working on the following fixes which will be available soon:

```
     AIX 3.2.x:  imapd not shipped (not vulnerable)

     AIX 4.1.x:  imapd not shipped (not vulnerable)

     AIX 4.2.x:  IX80446

     AIX 4.3.x:  IX80447

   To Order

   --------
```

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL: http://aix.software.ibm.com/aix.us/swfixes/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NetBSD

NetBSD does not ship the UW imapd daemon in its standard or development operating system releases. Our optional package system also does not include it at this time.

OpenBSD

OpenBSD has never shipped an imap daemon.

Red Hat Linux

Serious security problems have been found in all versions of imap shipped with Red Hat Linux. If "rpm -q imap" shows that imap is installed on your system, please upgrade to these new imap releases immediately, or remove imap by running "rpm -e imap". Note that Red Hat's imap package also provides a POP server, so only remove it if you don't need to provide POP services.

Thanks to everyone who helped find these problems, Olaf Kirch in particular.

```
   Red Hat 5.0 and 5.1

   -------------------

   i386:

   rpm -Uvh ftp://ftp.redhat.com/updates/5.0/i386/imap-4.1.final-
1.i386.rp

   alpha:

   rpm -Uvh ftp://ftp.redhat.com/updates/5.0/alpha/imap-4.1.final-
1.alpha.rp

   SPARC:

   rpm -Uvh ftp://ftp.redhat.com/updates/5.0/sparc/imap-4.1.final-
1.sparc.rpm


   Red Hat 4.2

   ----------

   i386:

   rpm -Uvh ftp://ftp.redhat.com/updates/4.2/i386/imap-4.1.final-
0.i386.rpm

   alpha:
```

```
   rpm -Uvh ftp://ftp.redhat.com/updates/4.2/alpha/imap-4.1.final-
0.alpha.rp

   SPARC:

   rpm -Uvh ftp://ftp.redhat.com/updates/4.2/sparc/imap-4.1.final-
0.sparc.rpm
```

The Santa Cruz Operation, Inc.

The following SCO products are vulnerable:

- SCO UnixWare 7

SCO OpenServer 5.0, SCO CMW+ 3.0, SCO Open Desktop/Open Server 3.0,   and UnixWare 2.1 is not vulnerable as University of Washington imapd is not included in these platforms. Binary versions of University of Washington imapd will be available shortly from the SCO ftp site:

ftp://ftp.sco.com/SSE/sse014.ltr - cover letter

ftp://ftp.sco.com/SSE/sse014.tar.Z - replacement binaries

This fix is a binary for the following SCO operating systems:

- SCO UnixWare 7

For the latest security bulletins and patches for SCO products, please refer to http://www.sco.com/security/.

Silicon Graphics Inc.

Please refer to Silicon Graphics Inc. Security Advisory, "University of Washington imapd daemon Vulnerability," Number: 19980802-01-I, distributed August 6, 1998 for additional information relating to this vulnerability.

The primary SGI anonymous FTP site for security information and patches is sgigate.sgi.com (204.94.209.1). Security information and patches are located under the directories ~ftp/security and ~ftp/patches, respectively. The Silicon Graphics Security Headquarters Web page is accessible at the URL http://www.sgi.com/Support/security/security.html.

The CERT Coordination Center thanks Olaf Kirch of Caldera Linux for discovering and reporting the vulnerability. Additionally, we would like to thank Mark Crispin and Lori Stevens of the University of Washington for providing technical details and support in the development of the advisory.

Revision History

Mar. 08, 1999 Updated IMAP Server information for ISOCOR.

Nov. 16, 1998 Updated patch information for Sun Microsystems, Inc.

Sept. 4, 1998 Added vendor information for Silicon Graphics, Inc.

Aug. 14, 1998 Added vendor information for Microsoft Corporation.

10 CA-1998-10: Buffer Overflow in MIME-aware Mail and News Clients

Original issue date: August 11, 1998
Last revised: October 19, 1998
Added vendor information for Compaq Computer Corporation

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

The CERT Coordination Center has received reports of a vulnerability in some MIME-aware mail and news clients.

The CERT/CC team recommends updating any vulnerable mail or news clients according to the information provided in Appendix A. In addition, network administrators may be able to employ some risk mitigation strategies until they are able to update all the vulnerable clients. These strategies are described in Appendix B.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

As of the publication date of this advisory, we have not received any reports indicating this vulnerability has been successfully exploited.

I. Description

A vulnerability in some MIME-aware mail and news clients could allow an intruder to execute arbitrary code, crash the system, or gain administrative rights on vulnerable systems. The vulnerability has been discovered by Marko Laakso and Ari Takanen of the Secure Programming Group of the University of Oulu. It has received considerable public attention in the media and through reports published by Microsoft, Netscape, AUSCERT, CIAC, NTBugTraq, and others.

The vulnerability affects a number of mail and news clients in addition to the ones which have been the subjects of those reports.

II. Impact

An intruder who sends a carefully crafted mail message to a vulnerable system can, under some circumstances, cause code of the intruder's choosing to be executed on the vulnerable system. Additionally, an intruder can cause a vulnerable mail program to crash unexpectedly. Depending on the operating system on which the mail client is running and the privileges of the user running the vulnerable mail client, the intruder may be able to crash the entire system. If a privileged user reads mail with a vulnerable mail user agent, an intruder can gain administrative access to the system.

III. Solution

A. Obtain and install a patch for this problem as described in Appendix A.

B. Until you are able to install the appropriate patch, you may wish to install patches to sendmail or to use procmail filtering as described in Appendix B.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Caldera Inc.

Caldera is currently investigating these issues and in the process of releasing a fix. Updated RPMs will be uploaded to:

> ftp://ftp.caldera.com/pub/OpenLinux/updates/1.2/011
> 9d2a8ca516c3bbbe920a72d365780fe3 mutt-0.93.1-2.i386.rpm
> a20383c9c6f73aac56731ab65c9525fd mutt-0.93.1-2.src.rpm

Compaq Computer Corporation

```
SOURCE:

(c) Copyright 1994, 1995, 1996, 1997, 1998 Compaq Computer Corpora-
tion.

All rights reserved.

SOURCE: Compaq Computer Corporation

        Compaq Services

        Software Security Response Team USA

X-REF:  AUSCERT AA-98.04,

        CIAC I-077,

        CERT CA-98.10

Subj.   mime-aware mail clients

This reported problem is not present for the as shipped, Compaq's
Digital ULTRIX or Compaq's Digital UNIX Operating Systems Software.

- Compaq Computer Corporation
```

Data General Corporation

DG/UX is not vulnerable to this report as it includes no native utilities with mime support.

Fujitsu

Fujitsu's operating system, UXP/V, does not support any mail client which can handle MIME encoding/decoding. Therefore, Fujitsu UXP/V is not vulnerable.

Hewlett-Packard Company

The version of dtmail supplied by HP, as part of HP's CDE product, is vulnerable. Patches in process.

Iris

Iris is aware of this problem and is investigating to determine if Lotus Notes is vulnerable.

Microsoft Corporation

Previously released information regarding this vulnerability is available from Microsoft at http://www.microsoft.com/security/bulletins/ms98-008.htm.

Mutt

Mutt versions up to 0.93.1(i) were vulnerable to a remotely exploitable buffer overflow. The bug has been fixed as of mutt 0.93.2(i). A patch was distributed on Usenet on July 29.

Users of older versions should upgrade as soon as possible.

Mutt 0.93.2(i) is available from ftp://ftp.guug.de/pub/mutt/.

The distribution files with their MD5 checksums:

```
diff-0.93.1-0.93.2.gz 39918e8c27e1a762af77052ea1164dbb
diff-0.93.1i-0.93.2i.gz aa08b3b3ade6e733c9bb01809199e3e7
mutt-0.93.2i.tar.gz 9ce8f1020a638d07cb3772b1ebe9887d
mutt-0.93.2.tar.gz 89a0888b1d25895cdc74f0999713f52b
```

SHA1 checksums:

```
diff-0.93.1-0.93.2.gz 326b4dd8479717ab1bc073a1a3eaa13ef6d551df
diff-0.93.1i-0.93.2i.gz 1358d1462d76c1c41a2070bdf5eee1b60a216ee8
mutt-0.93.2i.tar.gz 2a16bd1ee9edf24222d39998e80d8adafa6d45fa
mutt-0.93.2.tar.gz 1048f600395b328783bf58dedddd9a18ad4e36d1
```

Credits for noting this bug and giving a first fix on bugtraq go to Paul Boehm <paul@boehm.org>.

NCR

No products are affected.

NetBSD Foundation

The NetBSD Foundation package system contains packages for mutt and pine. All users should upgrade to the latest version of these packages as soon as possible. Updated binary packages will become available on the NetBSD FTP server as soon as possible, and will be announced on the netbsd-announce@netbsd.org list. To join this list, or more information about NetBSD, please see http://www.NetBSD.ORG/.

Netscape

Previously released information regarding this vulnerability is available from Netscape at http://www.netscape.com/products/security/resources/bugs/longfile.html

OpenBSD

Not affected. OpenBSD does not ship any of the affected products.

Pegasus Mail

We have conducted a strenuous examination of the equivalent code in Pegasus Mail and can confirm that Pegasus Mail is *not* vulnerable to this particular attack. Pegasus Mail handles attachments in a different manner from the affected Netscape and Microsoft products, and does proper bounds checking on filename lengths in all cases.

In the course of following up on this problem, we *have* unearthed a related problem, though: there are conceivable scenarios where Pegasus Mail may be made to crash when it attempts to parse a particular class of improperly-formatted MIME headers. The crash does not result from a buffer overflow, and hence has none of the security ramifications of the Netscape/OE problem - the crash itself is the worst that can happen. We have corrected this particular parser problem for the v3.01c release of Pegasus Mail, which will be out early next week.

To reiterate: Pegasus Mail is *not* vulnerable to the problem currently being publicized.

Mercury users: our Mercury Mail Transport System is not currently required to perform MIME parsing, and is hence completely immune to this problem.

QUALCOMM Incorporated

Eudora Pro Email, Eudora Pro CommCenter and Eudora Light not susceptible to buffer overflow security problem

QUALCOMM tested its line of Eudora email software after becoming aware of the buffer overflow security problems recently found in Microsoft and Netscape email programs. QUALCOMM is pleased to announce that its Eudora email products are not susceptible to the types of attacks that can harm the computers of users of these other products. QUALCOMM tested the latest versions of Eudora Pro and Eudora CommCenter versions 4.0, 4.0.1 and 4.1 (beta), as well as Eudora Pro and Eudora Light versions 3.0 through 3.0.5 (Windows) and 3.1.3 (Mac). In all cases, Eudora does not allow any unauthorized programs to be automatically executed on a user's system by exploiting buffer overflow flaws.

Internally, Eudora 4.0.1 (shipping) and 4.1 (beta) checks incoming header sizes and in particular attachment name lengths and truncates where appropriate to avoid buffer overrun. Previous versions of Eudora, specifically the Windows Eudora versions 3.0 through 3.0.5 and 4.0, long attachment names under certain conditions could cause the program to terminate prematurely, but most importantly, not in such a way as to allow unauthorized execution of code. Upgrading to Windows Eudora 4.0.1 or 4.0.2 (both shipping) or 4.1 (beta) resolves that particular issue.

An unrelated security issue has recently been made public regarding the use of Java scripts and attachments in email messages received by Eudora 4.x. Full details of this issue, along with links to Eudora Pro 4.0.2 and 4.1 updaters is available at http://eudora.qualcomm.com/security.html. The available Eudora Pro 4.0.2 and 4.1 updaters correct the potential security risk.

The Santa Cruz Operation, Inc. (SCO)

The following SCO products are not vulnerable:
- - SCO CMW+
- - SCO Open Desktop / Open Server 3.0, SCO UNIX 3.2v4
- - SCO OpenServer 5, SCO Internet FastStart
- - SCO UnixWare 2.1

SCO UnixWare 7 dtmail may be vulnerable - investigation is continuing. Pending this investigation, SCO recommends that dtmail not be used on UnixWare 7; mail may be safely read using mailx or Netscape Navigator.

Sun Microsystems, Inc.

Please refer to Sun Microsystems, Inc. Security Bulletin, "mailtool", Number: 00175, distributed September 9, 1998 for additional information relating to this vulnerability.

Patches and Checksums are available to all Sun customers via World Wide Web at:
http://sunsolve.sun.com/sunsolve/pubpatches/patches.html.

Sun security bulletins are available via World Wide Web at:
http://sunsolve.sun.com/pub-cgi/secbul.pl.

University of Washington

Pursuant to recent reports of vulnerability to mal-formed or malicious MIME attachments, the UW Pine Team has corrected a few cases of potential buffer overrun in the latest Pine Message

System release, version 4.02, that might cause Pine to crash when inordinately long MIME-header information is encountered.

It has been speculated that these problems could be exploited to allow a message sender to execute an arbitrary command on behalf of the receiving user, although with no more privilege than the receiving user. While the UW Pine Team is not aware of any specific attacks involving this bug, they have made a source patch available to address this threat.

The source patch is available from: ftp://ftp.cac.washington.edu/pine/pine4.02A.patch.

Or via links found within the Pine Information Center at: http://www.washington.edu/pine/.

The patch is intended for the Pine Mail System version 4.02 (released 21 July 1998). The file is in context-diff format, and should be understood by the "patch" utility. To update Pine 4.02 source, simply copy the patch file into the same directory as the pine4.02 source tree and type:

```
patch -p < pine4.02A.patch
```

The UW Pine Team strongly encourages sites running version 4.00 or greater to upgrade to the latest release, and apply the published patch. While versions prior to 4.00 are less sensitive to malicious messages, upgrading to version 4.02A (including the patch) is recommended.

Appendix B Risk Mitigation

Although the vulnerability described in this advisory affects mail user agents, it may be possible to reduce the risk by modifying mail transfer agents to detect the vulnerability before it reaches the mail user agent, or by filtering the message. Below is a list of vendors who have provided us information on strategies that can mitigate the risk. Note that these vendors are not themselves vulnerable to this problem.

Sendmail, Inc.

Sendmail, Inc. has produced a patch for version 8.9.1 of sendmail as a service to their user base to assist system administrators in proactively defending against these problems. Sites who choose not to install the patch at this time will not increase their exposure to the problem in this case. This patch and installation instructions are available at http://www.sendmail.com/sendmail.8.9.1a.html.

Note that the patch is specific to sendmail version 8.9.1 only. If you are unable to upgrade to this version, do not attempt to use the patch.

John Hardin

John Hardin has modified his procmail Filters Kit to include filters which may be able to assist sites in defending against these problems. More information about the procmail Filters Kit is available at http://www.wolfenet.com/~jhardin/procmail-security.html.

Our thanks go to Marko Laakso and Ari Takanen of the Secure Programming Group of the University of Oulu; Eric Allman and Gregory Shapiro of Sendmail, Inc; AUSCERT; DFN-CERT; John Hardin; and Gene Spafford of Purdue University for their input.

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.

Revision History

Oct. 19, 1998	Added vendor information for Compaq Computer Corporation
Sept. 18, 1998	Added vendor information for Sun Microsystems, Inc.
Aug. 12, 1998	Added vendor information, see Appendix A
	Updated risk mitigation information, see Appendix B
Aug. 11, 1998	Updated vendor information for Pegasus Mail

11 CA-1998-11: Vulnerability in Tooltalk RPC Service

Original issue date: September 3, 1998
Last revised: July 22, 1999
Added link IN-99-04 to the "Updates" section.

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

The text of this advisory was originally released on August 31, 1998, as NAI-29, developed by Network Associates, Inc. (NAI). To more widely broadcast this information, we are reprinting the NAI advisory here with their permission.

As we receive additional information it will be placed in an "Updates" section at the end of this advisory.

Stack Overflow in ToolTalk RPC Service

NAI Advisory 29

Network Associates, Inc.

SECURITY ADVISORY

August 31, 1998

SYNOPSIS

An implementation fault in the ToolTalk object database server allows a remote attacker to run arbitrary code as the superuser on hosts supporting the ToolTalk service. The affected program runs on many popular UNIX operating systems supporting CDE and some Open Windows installs. This vulnerability is being actively exploited by attackers on the Internet.

Confirmed Vulnerable Operating Systems and Third Party Vendors

Sun Microsystems

SunOS 5.6, 5.6_x86
SunOS 5.5.1, 5.5.1_x86
SunOS 5.5, 5.5_x86
SunOS 5.4, 5.4_x86
SunOS 5.3
SunOS 4.1.
SunOS 4.1.3_U1

Hewlett Packard

HP-UX release 10.10
HP-UX release 10.20
HP-UX release 10.30
HP-UX release 11.00

SGI

IRIX 5.3
IRIX 5.4
IRIX 6.2
IRIX 6.3
IRIX 6.4

IBM

AIX 4.1.X
AIX 4.2.X
AIX 4.3.X

TriTeal

TriTeal CDE - TED versions 4.3 and previous.

Xi Graphics

Xi Graphics Maximum CDE v1.2.3

It should be noted here that this not an exhaustive list of vulnerable vendors. These are only the *confirmed vulnerable* vendors. Also, any OS installation that is not configured to use or start up the ToolTalk service is not vulnerable to this problem. To determine whether the ToolTalk database server is running on a host, use the "rpcinfo" command to print a list of the RPC services running on it, as:

```
$ rpcinfo -p hostname
```

Because many operating systems do not include an entry for the ToolTalk database service in the RPC mapping table ("/etc/rpc" on most Unix platforms), the vulnerable service may not appear by name in the listing. The RPC program number for the ToolTalk database service is 100083. If an entry exists for this program, such as,

```
100083 1 tcp 692
```

then the service is running on the host. Until additional information is made available from the OS vendor, it should be assumed that the system is vulnerable to the attack described in this advisory.

DETAILS

The ToolTalk service allows independently developed applications to communicate with each other by exchanging ToolTalk messages. Using ToolTalk, applications can create open protocols which allow different programs to be interchanged, and new programs to be plugged into the system with minimal reconfiguration.

The ToolTalk database server (rpc.ttdbserverd) is an ONC RPC service which manages objects needed for the operation of the ToolTalk service. ToolTalk-enabled processes communicate with each other using RPC calls to this program, which runs on each ToolTalk-enabled host. This program is a standard component of the ToolTalk system, which ships as a standard component of many commercial Unix operating systems. The ToolTalk database server runs as root.

Due to an implementation fault in rpc.ttdbserverd, it is possible for a malicious remote client to formulate an RPC message that will cause the server to overflow an automatic variable on the stack. By overwriting activation records stored on the stack, it is possible to force a transfer of control into arbitrary instructions provided by the attacker in the RPC message, and thus gain total control of the server process.

TECHNICAL DETAILS

Source code and XDR specifications for the ToolTalk database protocol and server were not available at the time this advisory was drafted. What follows is information based on analysis of the rpc.ttdbserverd binary and a captured attack trace from a network on which an exploitation script for this problem was run.

The observed attack utilized the ToolTalk Database (TTDB) RPC procedure number 7, with an XDR-encoded string as its sole argument. TTDB procedure 7 corresponds to the _tt_iserase_1() function symbol in the Solaris binary (/usr/openwin/bin/rpc.ttdbserverd). This function implements an RPC procedure which takes an ASCII string as an argument, which is treated as a pathname.

The pathname string is passed to the function isopen(), which in turn passes it to _am_open(), then to _amopen(), _openfcb(), _isfcb_open(), and finally to _open_datfile(), where it, as the first argument to the function, is passed directly to a strcpy() to a pointer on the stack. If the pathname string is suitably large, the string overflows the stack buffer and overwrites an activation record, allowing control to transfer into instructions stored in the pathname string.

RESOLUTION

This is an implementation problem and can only be resolved completely by applying patches to or replacing affected software. As a temporary workaround, it is possible to eliminate vulnerability to this problem by disabling the ToolTalk database service. This can be done by killing the "rpc.ttdbserverd" process and removing it from any OS startup scripts. It should be noted that this may impair system functionality.

The following vendors have been confirmed vulnerable, contacted, and have responded with repair information:

Sun Microsystems

Sun plans to release patches this week that relate to the ToolTalk vulnerability for SunOS 5.6, 5.6_x86, 5.5.1, 5.5.1_x86, 5.5 and 5.5_x86.

Patches for SunOS 5.4, 5.4_x86, 5.3, 4.1.4 and 4.1.3_U1 will be released in about 4 weeks.

Sun recommended security patches (including checksums) are available from: http://sunsolve.sun.com/sunsolve/pubpatches/patches.html

Hewlett Packard

HP-UX has been confirmed vulnerable in releases 10.XX and 11.00. HP has made patches available with the following identifications:

HP-UX release 10.10 HP9000 Series 7/800 PHSS_16150
HP-UX release 10.20 HP9000 Series 7/800 PHSS_16147
HP-UX release 10.24 HP9000 Series 7/800 PHSS_16197
HP-UX release 10.30 HP9000 Series 7/800 PHSS_16151
HP-UX release 11.00 HP9000 Series 7/800 PHSS_16148

IBM

IBM AIX has been confirmed vulnerable. IBM's response is as follows:

The version of ttdbserver shipped with AIX is vulnerable. We are currently working on the following fixes which will be available soon:

```
APAR 4.1.x: IX81440
```

```
APAR 4.2.x: IX81441
```

```
APAR 4.3.x: IX81442
```

Until the official APARs are available, a temporary fix can be downloaded via anonymous ftp from: ftp://aix.software.ibm.com/aix/efixes/security/ttdbserver.tar.Z.

TriTeal

An official response from TriTeal is as follows:

The ToolTalk vulnerability will be fixed in the TED4.4 release. For earlier versions of TED, please contact the TriTeal technical support department at support@triteal.com or at http://www.triteal.com/support.

Xi Graphics

An official response from Xi Graphics is as follows:

Xi Graphics Maximum CDE v1.2.3 is vulnerable to this attack. A patch to correct this problem will be placed on our FTP site by 8/28/1998:

- ftp://ftp.xig.com:/pub/updates/cde/1.2.3/C1203.002.tar.gz
- ftp://ftp.xig.com:/pub/updates/cde/1.2.3/C1203.002.txt

Users of Maximum CDE v1.2.3 are urged to install this update.

Silicon Graphics

Please refer to Silicon Graphics Inc. Security Advisory, "Vulnerability in ToolTalk RPC Service," Number: 19981101-01-A, distributed November 19, 1998 for additional information relating to this vulnerability.

The primary SGI anonymous FTP site for security information and patches is sgigate.sgi.com (204.94.209.1). Security information and patches are located under the directories ~ftp/security and ~ftp/patches, respectively. The Silicon Graphics Security Headquarters Web page is accessible at the URL http://www.sgi.com/Support/security/security.html.

Other Vendors

If any uncertainty exists with regards to whether a given vendor not listed in this advisory is vulnerable to this attack, we recommend contacting them via their support/security channels for more information.

ACKNOWLEDGEMENTS

The NAI Security Labs Team would like to thank the HP & IBM Security Response Teams, CERT/CC & AUSCERT for their contributions to this advisory.

ABOUT THE NETWORK ASSOCIATES SECURITY LABS

The Security Labs at Network Associates hosts some of the most important research in computer security today. With over 28 published security advisories published in the last 2 years, the Network Associates security auditing teams have been responsible for the discovery of many of the Internet's most serious security flaws. This advisory represents our ongoing commitment to provide critical information to the security community.

For more information about the Security Labs at Network Associates, see our website at http://www.nai.com or contact us at seclabs@nai.com.

UPDATES

For more information about attacks using various RPC Services please see CERT® Incident Note IN-99-04 http://www.cert.org/incident_notes/IN-99-04.html.

Revision History

```
July 22, 1999  Added link IN-99-04 to the "Updates" section.

Dec.  9, 1998  Updated RESOLUTION information for Silicon Graphics.

Sept. 4, 1998  Updated RESOLUTION information for Hewlett Packard.
```

12 CA-1998-12: Remotely Exploitable Buffer Overflow Vulnerability in mountd

Original issue date: October 12, 1998
Last revised: November 9, 1998
Added vendor information for IBM Corporation and Silicon Graphics Inc.
Updated information for Data General

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

Systems Affected

NFS servers running certain implementations of mountd, primarily Linux systems. On some systems, the vulnerable NFS server is enabled by default. This vulnerability can be exploited even if the NFS server does not share any file systems.

See Appendix A for information from vendors. If your vendor's name does not appear, we did not hear from that vendor.

Overview

NFS is a distributed file system in which clients make use of file systems provided by servers. There is a vulnerability in some implementations of the software that NFS servers use to log requests to use file systems.

When a client makes a request to use a file system and subsequently makes that file system available as a local resource, the client is said to "mount" the file system. The vulnerability lies in the software on the NFS server that handles requests to mount file systems. This software is usually called "mountd" or "rpc.mountd."

Intruders who exploit the vulnerability are able to gain administrative access to the vulnerable NFS file server. That is, they can do anything the system administrator can do. This vulnerability can be exploited remotely and does not require an account on the target machine.

On some vulnerable systems, the mountd software is installed and enabled by default. See Appendix A for more information.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

NFS is used to share files among different computers over the network using a client/server paradigm. When an NFS client computer wishes to access files on an NFS server, the client must first make a request to mount the file system. There is a vulnerability in some implementations of the software that handles NFS mount requests (the mountd program). Specifically, it is possible for an intruder to overflow a buffer in the area of code responsible for logging NFS activity.

We have received reports indicating that intruders are actively using this vulnerability to compromise systems and are engaging in large-scale scans to locate vulnerable systems.

On some systems, the vulnerable NFS server is enabled by default. See the vendor information in Appendix A.

II. Impact

After causing a buffer overflow, a remote intruder can use the resulting condition to execute arbitrary code with root privileges.

III. Solution

A. Install a patch from your vendor.

Appendix A contains input from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

B. Until you install a patch, use the following workaround.

Consider disabling NFS until you are able to install the patch. In particular, since some systems have vulnerable versions of mountd installed and enabled by default, we recommend you disable mountd on those systems unless you are actively using those systems as NFS servers.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSDI systems are not vulnerable to this attack.

Caldera

Caldera provided a fixed version as nfs-server-2.2beta35-2 on Aug 28. It is available from ftp://ftp.caldera.com/pub/OpenLinux/updates/1.2/013.

```
10fdb82ed8fd1b88c73fd962d8980bb4 RPMS/nfs-server-2.2beta35-
2.i386.rpm
59e275b1ed6b98a39a38406f0415a226 RPMS/nfs-server-clients-2.2beta35-
2.i386.rpm
```

```
6b075faf1d424e099c6932d95e76fd6b SRPMS/nfs-server-2.2beta35-
2.src.rpm
```

Compaq Computer Corporation

SOURCE: (c) Copyright 1994, 1995, 1996, 1997, 1998 Compaq Computer Corporation. All rights reserved.

SOURCE: Compaq Computer Corporation Compaq Services Software Security Response Team USA

x-ref: SSRT0574U mountd

This reported problem is not present for the as shipped, Compaq's Digital ULTRIX or Compaq's Digital UNIX Operating Systems Software.

- Compaq Computer Corporation

Data General Corporation

DG/UX is not vulnerable to this problem.

FreeBSD, Inc.

FreeBSD 2.2.6 and above seem not be vulnerable to this exploit.

Fujitsu Limited

Fujitsu's UXP/V operating system is not vulnerable.

Hewlett-Packard Company

Not vulnerable.

IBM Corporation

The version of rpc.mountd shipped with AIX is not vulnerable.

IBM and AIX are registered trademarks of International Business Machines Corporation.

NCR

NCR is not vulnerable. We do not do any of the specified logging, nor do we have mountd (or normally anything else) hanging on port 635.

The NetBSD Project

NetBSD is not vulnerable to this attack in any configuration. Neither the NFS server or mount daemon are enabled by default.

The OpenBSD Project

OpenBSD is not affected.

Red Hat Software, Inc.

All versions of Red Hat Linux are vulnerable, and we have provided fixed packages for all our users. Updated nfs-server packages are available from our site at http://www.redhat.com/support/docs/errata.html

The Santa Cruz Operation, Inc.

No SCO platforms are vulnerable.

Silicon Graphics Inc.

Please refer to Silicon Graphics Inc. Security Advisory, "mountd Buffer Overflow Vulnerability", Number: 19981006-01-I, distributed October 26, 1998 for additional information about this vulnerability.

Silicon Graphics provides a comprehensive customer World Wide Web site. This site is located at http://www.sgi.com/Support/security/security.html

Sun Microsystems, Inc.

Sun's mountd is not affected.

Contributors

Our thanks to Olaf Kirch and Wolfgang Ley for their input and assistance in constructing this advisory.

Revision History

```
Nov.  9, 1998  Added vendor information for IBM and SGI

               Updated information for Data General
```

```
Oct. 21, 1998  Added vendor information for Berkeley Software De-
sign, Inc.
```

13 CA-1998-13: Vulnerability in Certain TCP/IP Implementations

Original issue date: December 21, 1998
Last revised: --

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

Systems Affected

Some systems with BSD-derived TCP/IP stacks. See Appendix A for a complete list of affected systems.

Overview

Intruders can disrupt service or crash systems with vulnerable TCP/IP stacks. No special access is required, and intruders can use source-address spoofing to conceal their true location.

I. Description

By carefully constructing a sequence of packets with certain characteristics, an intruder can cause vulnerable systems to crash, hang, or behave in unpredictable ways. This vulnerability is similar in its effect to other denial-of-service vulnerabilities, including the ones described in http://www.cert.org/advisories/CA-97.28.Teardrop_Land.html.

Specifically, intruders can use this vulnerability in conjunction with IP-source-address spoofing to make it difficult or impossible to know their location. They can also use the vulnerability in conjunction with broadcast packets to affect a large number of vulnerable machines with a small number of packets.

II. Impact

Any remote user can crash or hang a vulnerable machine, or cause the system to behave in unpredictable ways.

III. Solution

A. Install a patch from your vendor.

Appendix A contains input from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

B. Configure your router or firewall to help prevent source-address spoofing.

We encourage sites to configure their routers or firewalls to reduce the ability of intruders to use source-address spoofing. Currently, the best method to reduce the number of IP-spoofed packets exiting your network is to install filtering on your routers that requires packets leaving your network to have a source address from your internal network. This type of filter prevents a source IP-spoofing attack from your site by filtering all outgoing packets that contain a source address of a different network.

A detailed description of this type of filtering is available in RFC 2267, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" by Paul Ferguson of Cisco Systems, Inc. and Daniel Senie of Blazenet, Inc. We recommend it to both Internet Service Providers and sites that manage their own routers. The document is currently available at http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2267.txt.

Note that this type of filtering does not protect a site from the attack itself, but it does reduce the ability of intruders to conceal their location, thereby discouraging attacks.

Appendix A Vendor Information

Berkeley Software Design, Inc. (BSDI)

BSDI's current release BSD/OS 4.0 is not vulnerable to this problem. BSD/OS 3.1 is vulnerable and a patch (M310-049) is available from BSDI's WWW server at http://www.bsdi.com/support/patches or via our ftp server from the directory ftp://ftp.bsdi.com/bsdi/patches/patches-3.1.

Cisco Systems

Cisco is not vulnerable.

Compaq Computer Corporation

SOURCE: (c) Copyright 1994, 1995, 1996, 1997, 1998 Compaq Computer Corporation.

All rights reserved.

SOURCE: Compaq Computer Corporation
Compaq Services
Software Security Response Team USA

This reported problem is not present for the as shipped, Compaq's Digital ULTRIX or Compaq's Digital UNIX Operating Systems Software.

- Compaq Computer Corporation

Data General Corporation

We are investigating. We will provide an update when our investigation is complete.

FreeBSD, Inc.

FreeBSD 2.2.8 is not vulnerable.
FreeBSD versions prior to 2.2.8 are vulnerable.
FreeBSD 3.0 is also vulnerable.
FreeBSD 3.0-current as of 1998/11/12 is not vulnerable.

A patch is available at ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/CA-98-13/patch.

Fujitsu

Regarding this vulnerability, Fujitsu's UXP/V operating system is not vulnerable.

Hewlett-Packard Company

HP is not vulnerable.

IBM Corporation

AIX is not vulnerable.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Livingston Enterprises, Inc.

Livingston systems are not vulnerable.

Computer Associates International

CA systems are not vulnerable.

Microsoft Corporation

Microsoft is not vulnerable.

NEC Corporation

NEC Corporation EWS-UX, UP-UX and UX/4800 Unix systems are not vulnerable to this problem.

OpenBSD

Security fixes for this problem are now available for 2.3 and 2.4.

For 2.3, see www.openbsd.org/errata23.html#tcpfix. For our 2.4 release which is available on CD on Dec 1, see www.openbsd.org/errata.html#tcpfix. The bug is fixed in our -current source tree.

Sun Microsystems, Inc.

We have confirmed that SunOS and Solaris are not vulnerable to the DOS attack.

Wind River Systems, Inc.

We've taken a look at our networking code and have determined that this is not a problem in the currently shipping version of the VxWorks RTOS.

Contributors

The vulnerability was originally discovered by Joel Boutros of the Enterprise Security Services team of Cambridge Technology Partners. Guido van Rooij of FreeBSD, Inc., provided an analysis of the vulnerability and information regarding its scope and extent.

Revision History