CERT Advisory CA-1996-26 Denial-of-Service Attack via ping

Original issue date: December 18, 1996
Last revised: December 5, 1997
Updated information for NCR Corporation.

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

The CERT Coordination Center has received reports of a denial-of-service attack using large ICMP datagrams. Exploitation details involving this vulnerability have been widely distributed.

The CERT/CC team recommends installing vendor patches as they become available.

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

I. Description

The TCP/IP specification (the basis for many protocols used on the Internet) allows for a maximum packet size of up to 65536 octets (1 octet = 8 bits of data), containing a minimum of 20 octets of IP header information and 0 or more octets of optional information, with the rest of the packet being data. It is known that some systems will react in an unpredictable fashion when receiving oversized IP packets. Reports indicate a range of reactions including crashing, freezing, and rebooting.

In particular, the reports received by the CERT Coordination Center indicate that Internet Control Message Protocol (ICMP) packets issued via the "ping" command have been used to trigger this behavior. ICMP is a subset of the TCP/IP suite of protocols that transmits error and control messages between systems. Two specific instances of the ICMP are the ICMP ECHO_REQUEST and ICMP ECHO_RESPONSE datagrams. These two instances can be used by a local host to determine whether a remote system is reachable via the network; this is commonly achieved using the "ping" command.

Discussion in public forums has centered around the use of the "ping" command to construct oversized ICMP datagrams (which are encapsulated within an IP packet). Many ping implementations by default send ICMP datagrams consisting only of the 8 octets of ICMP header information but allow the user to specify a larger packet size if desired.

You can read more information about this vulnerability on Mike Bremford's Web page. (Note that this is not a CERT/CC maintained page. We provide the URL here for your convenience.)

http://www.sophist.demon.co.uk/ping/index.html

II. Impact

Systems receiving oversized ICMP datagrams may crash, freeze, or reboot, resulting in denial of service.

III. Solution

First, since crashing a router or firewall may be part of a larger, multistage attack scenario, we encourage you to inspect the running configuration of any such systems that have crashed to ensure that the configuration information is what you expect it to be.

Then install a patch from your vendor.

Below is a list of vendors who have provided information about patches for this problem. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Computer Associates, Intl. (products for NCR)
Cray Research
Digital Equipment Corporation
Free BSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux Systems
NCR Corporation
NEC Corporation
Open Software Foundation (OSF)
The Santa Cruz Operation, Inc. (SCO)
Sun Microsystems, Inc.

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, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
BSD/OS 2.1 is not vulnerable to this problem. It correctly handles large packets without any problems.

Computer Associates, Intl.
(products for NCR)

Not vulnerable.

Cray Research
Attempts to send oversized ICMP datagrams are rejected with appropriate error messages. We believe that oversized ICMP datagrams sent to Unicos systems will also be rejected without crashing.

Data General Corporation
Due to the way DG/UX processes tcp packets, DG/UX is not vulnerable to this attack.

Digital Equipment Corporation
MSG ID: SSRT0429 From DSNlink/DIA Database

The following is important information concerning a potential denial of service issue which affects Digital UNIX Operating System, Digital UNIX MLS+, Firewall implementations, and Digital TCP/IP Services for OpenVMS AXP & VAX

```
COMPONENT:  System Security / Potential Denial of Service

  DIGITAL UNIX     Version: 3.0, 3.0b, 3.2, 3.2c, 3.2de1, 3.2de2,
                            3.2f, 3.2g, 4.0, 4.0a
  DIGITAL UNIX MLS+ Version 3.1a
  DIGITAL TCP/IP Services for OpenVMS AXP & VAX Versions - 4.0, 4.1
  DIGITAL ULTRIX Versions 4.3, 4.3a, 4.4, 4.5
  DIGITAL Firewall for UNIX
  DIGITAL AltaVista Firewall for UNIX
  DIGITAL VAX/ELN
```

For more information check the DSNlink/DIA Articles (keyword PING), or the URL http://www.service.digital.com/html/whats-new.html for the latest information.

ADVISORY INFORMATION:

Digital recently discovered a potential denial of service issue that may occur by remote systems exploiting a recently published problem while executing the 'ping' command. Solutions and initial communications began appearing in DSNlink/DIA FLASH/articles in late October, 1996.

SEVERITY LEVEL: High.

SOLUTION:

Digital has reacted promptly to this reported problem and a complete set of patch kits are being prepared for all currently supported platforms.

The Digital patches may be obtained from your local Digital support channel or from the URL listed above. Please refer to the applicable README notes information prior to the installation of patch kits on your system.

DIGITAL EQUIPMENT CORPORATION

Free BSD, Inc.
We have fixed the problem in 2.1.6 and -current.

Hewlett-Packard Company
For HP9000 Series 700 and 800 systems, apply the appropriate patch. See Hewlett-Packard Security Bulletin #000040 (HPSBUX9610-040) for further details. The bulletin is available from the HP SupportLine and ftp://ftp.cert.org/pub/vendors/hp/

```
Patch Name(Platform/OS)   | Notes
--------------------------+---------------------------------
PHNE_9027 (s700 9.01)     : PHNE_7704 must first be installed
PHNE_9028 (s700 9.03/5/7) : PHNE_7252 must first be installed
PHNE_9030 (s700 10.00)    :             No patch dependencies
PHNE_9032 (s700 10.01)    : PHNE_8168 must first be installed
PHNE_9034 (s700 10.10)    : PHNE_8063 must first be installed
PHNE_9036 (s700 10.20)    :             No patch dependencies
--------------------------+---------------------------------
PHNE_8672 (s800 9.00)     : PHNE_7197 must first be installed
PHNE_9029 (s800 9.04)     : PHNE_7317 must first be installed
PHNE_9031 (s800 10.00)    :             No patch dependencies
PHNE_9033 (s800 10.01)    : PHNE_8169 must first be installed
PHNE_9035 (s800 10.10)    : PHNE_8064 must first be installed
PHNE_9037 (s800 10.20)    :             No patch dependencies
--------------------------+---------------------------------
```

For our MPE operating system, patches are in process. Watch for the issuance of our MPE security bulletin.

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX59644 (PTF - U444227 U444232)

To determine if you have this PTF on your system, run the following command:

```
lslpp -lB U444227 U444232
```

AIX 4.1

Apply the following fix to your system:

APAR - IX59453

To determine if you have this APAR on your system, run the following command:

```
instfix -ik IX59453
```

Or run the following command:

```
lslpp -h bos.net.tcp.client
```

Your version of bos.net.tcp.client should be 4.1.4.16 or later.

AIX 4.2

Apply the following fix to your system:

APAR - IX61858

To determine if you have this APAR on your system, run the following command:

```
instfix -ik IX61858
```

Or run the following command:

```
lslpp -h bos.net.tcp.client
```

Your version of bos.net.tcp.client should be 4.2.0.6 or later.

IBM SNG Firewall

NOTE: The fixes in this section should ONLY be applied to systems running the IBM Internet Connection Secured Network Gateway (SNG) firewall software. They should be applied IN ADDITION TO the IBM AIX fixes listed in the previous section.

IBM SNG V2.1

APAR - IR33376 PTF UR46673

IBM SNG V2.2

APAR - IR33484 PTF UR46641

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 to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines

Linux Systems
We recommend that you upgrade your Linux 1.3.x and 2.0.x kernels to Linux 2.0.27. This is available from all the main archive sites such as

ftp://ftp.cs.helsinki.fi/pub/Software/Linux

Users wishing to remain with an earlier kernel version may download a patch from http://www.uk.linux.org/big-ping-patch. This patch will work with 2.0.x kernel revisions but is untested with 1.3.x kernel revisions.

Red Hat Linux has chosen to issue a 2.0.18 based release with the fix. Red Hat users should obtain this from

ftp://ftp.redhat.com/pub/redhat/redhat-4.0/updates/i386/kernel-2.0.18-6.i386.rpm >

NCR Corporation
For MP-RAS 3.00 and above, using TCP/IP as package name "inet", not vulnerable.

NEC Corporation

```
- ------------------------------------------------------------------------
       OS               Version        Status
- ------------------   ------------   -----------------------------------
EWS-UX/V(Rel4.0)     R1.x - R6.x    not vulnerable
EWS-UX/V(Rel4.2)     R7.x - R10.x   not vulnerable
EWS-UX/V(Rel4.2MP)   R10.x          not vulnerable
UP-UX/V              R1.x - R4.x    not vulnerable
UP-UX/V(Rel4.2MP)    R5.x - R7.x    not vulnerable
UX/4800              R11.x          not vulnerable
- ------------------------------------------------------------------------
```

NCR
see Computer Associates, Intl.

Open Software Foundation (OSF)
OSF's OSF/1 R1.3.3 maintenance release includes a solution for this problem.

The Santa Cruz Operation, Inc. (SCO)
The following SCO products are known to be vulnerable:

SCO OpenServer 5.0.0, 5.0.2
SCO Internet FastStart 1.0.0, 1.1.0
SCO Open Desktop 3.0
SCO TCP/IP 1.2.1 on SCO Unix System V/386 Release 3.2 Version 4.2

The symptoms encountered vary greatly and seem to be related to the type of network interface device being used. Support Level Supplement (SLS) OSS449 addresses this problem for the following releases:

SCO OpenServer 5.0.0, 5.0.2
SCO Internet FastStart 1.0.0, 1.1.0.

This Supplement is available at the following URLs:

ftp://ftp.sco.COM/SLS/oss449a.ltr (cover letter)
ftp://ftp.sco.COM/SLS/oss449a.Z (image)

The checksums are as follows:

```
sum -r
 ------
       oss449a.ltr:    28877   42
         oss449a.Z:    54558 1762

 MD5
 ---
       MD5 (oss449a.Z) = e8fc8a29dd59683ce5107f3b9b8d1169
       MD5 (oss449a.ltr) = d51ee1caf33edb86f4dbeb1733c99d86
```

If this SLS is ever updated, it will be noted at:

ftp://ftp.sco.COM/SLS/README

Should more information become available for either SCO's OpenServer or UnixWare products, SCO will provide updated information for this advisory.

If you need further assistance, SCO's Web page is at http://www.sco.COM.

Support requests from supported customers may be addressed to support@sco.COM , or you may contact SCO as follows:

USA/Canada: 6am-5pm Pacific Standard Time (PST)
1-408-425-4726 (voice)
1-408-427-5443 (fax)

Pacific Rim, Asia, and Latin American customers: 6am-5pm Pacific Standard Time (PST)
1-408-425-4726 (voice)
1-408-427-5443 (fax)

Europe, Middle East, Africa: 9am-5:00pm Greenwich Mean Time (GMT)
+44 1923 816344 (voice)
+44 1923 817781 (fax)

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

```
        103630-09 5.5.1
        103631-09 5.5.1_x86
        103169-12 5.5
        103170-12 5.5_x86
        101945-51 5.4
        101946-45 5.4_x86
```

The CERT Coordination Center staff thanks AUSCERT, the Australian Computer Emergency Response Team, and DFN-CERT, the German team, for their contributions to this advisory, and we thank Mike Bremford for permission to cite the information he has made available to the community.

Revision History

```
Dec. 5, 1997  Appendix A - Updated information for NCR Corporation.
Sep. 24,1997  Updated copyright statement
Aug. 7, 1997  Changed vendor information for Sun Microsystems to remove
              incorrect patch reference.
July 28, 1997 Added vendor information for Sun Microsystems.
Jan. 20, 1997 Appendix A - added information from Data General Corporation.
Jan. 14, 1997 Appendix A - modified SCO entry to include updated patch
              information.
```