CERT Advisory 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