CERT Advisory CA-1997-28 IP Denial-of-Service Attacks

Original issue date: December 16, 1997
Last revised: May 26, 1998
Updated vendor information for Sun Microsystems, Inc.

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

The CERT Coordination Center has received reports of two attack tools (Teardrop and Land) that are being used to exploit two vulnerabilities in the TCP/IP protocol. Both tools enable a remote user to cause a denial of service.

The CERT/CC team recommends installing patches from your vendor. Until you are able to do so, we urge you to use the workaround described in Section III.B. to reduce the likelihood of a successful attack using Land. There is no workaround for Teardrop.

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

In recent weeks there has been discussion on public mailing lists about two denial-of-service attack tools, Teardrop and Land. These attack tools have similar effects on some systems (namely, causing the victim machine to crash), but the tools exploit different vulnerabilities.

The CERT Coordination Center has received several reports of sites being attacked by either one or both of these tools. It is important to note that it may be necessary for a system administrator to apply separate patches, if they exist, for each attack tool.

Topic 1 - Teardrop

Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. Teardrop is a widely available attack tool that exploits this vulnerability.

Topic 2 - Land

Some implementations of TCP/IP are vulnerable to packets that are crafted in a particular way (a SYN packet in which the source address and port are the same as the destination--i.e., spoofed). Land is a widely available attack tool that exploits this vulnerability.

II. Impact

Topic 1 - Teardrop

Any remote user can crash a vulnerable machine.

Topic 2 - Land

Any remote user that can send spoofed packets to a host can crash or "hang" that host.

III. Solution

CERT/CC urges you to immediately apply vendor patches if they are available. You may have to apply different patches for each attack tool.

You may want to use the workaround for Land, so please review both Sections A and B below.

1. Consult your vendor

   Appendix A contains information from vendors who provided input 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.

   It is important to note that you may have to apply different patches for each attack tool.

1. Apply the following workaround (Land only)

   A workaround for the Land attack tool is to block IP-spoofed packets. This workaround does not apply to the Teardrop attack tool because the Teardrop attack does not rely on IP-spoofed packets.

   Attacks like those of the Land tool rely on the use of forged packets, that is, packets where the attacker deliberately falsifies the origin address. With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can reduce the likelihood of your site’s networks being used to initiate forged packets by filtering outgoing packets that have a source address different from that of your internal network.

   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 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 of Blazenet, Inc. 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

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)

No version of BSD/OS is vulnerable to Teardrop.

Patched versions of 2.1 and all 3.0 and 3.1 versions are also not vulnerable to Land.

Caldera Corporation

Topic 1 - Teardrop

Unless patched, Linux 2.0.x kernels prior to 2.0.32 are vulnerable. With the application of the kernel update described in Caldera Security Advisory SA-1997.29 (dated 3-Dec-1997), Caldera OpenLinux is not vulnerable. This Caldera advisory describes how to obtain and install the update and can be found at:

Other Caldera Security Advisories can be found at:
http://www.caldera.com/tech-ref/security/

Topic 2 - Land

There are no known reports of any version of the Linux kernel, including those shipping with Caldera OpenLinux, being vulnerable to this exploit.

Cisco Systems

Topic 1 - Teardrop

Not vulnerable.

Topic 2 - Land

IOS/7000 software, Catalyst 5xxx and 29xx LAN switches, BPX and IGX WAN switches and AXIS shelf appear to be vulnerable. PIX firewall and Centri firewall are not vulnerable.

For more information reference URL:

Digital Equipment Corporation

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

The FreeBSD Project

Topic 1 - Teardrop

CSRG 4.4 is not vulnerable.

Topic 2 - Land

No feedback.

Hewlett-Packard Corporation

HPSBUX9801-076
SECURITY BULLETIN: #00076, 21 January 1998

Description: Security Vulnerability with land on HP-UX

The problem can be fixed by applying the appropriate cumulative ARPA Transport patch mentioned below.
IBM Corporation
Topic 1 - Teardrop
AIX is not vulnerable.

Topic 2 - Land
AIX is not vulnerable.

Microsoft Corporation
Topic 1 - Teardrop
Windows NT 4.0 with SP 3 and post SP 3 fixes applied and Windows 95 with the appropriate patch are not vulnerable.
Patch information is available at URL: ftp://ftp.microsoft.com/bussys/winnt/kb/Q154/1/74.TXT

Topic 2 - Land
Windows NT 4.0 with the appropriate patch is not vulnerable.

Windows 95 without the WinSock 2.0 Update is not vulnerable.

NCR Corporation
Topic 1 - Teardrop
NCR MP-RAS TCP/IP implementation is not vulnerable.

Topic 2 - Land
Apply a patch for your MP-RAS UNIX TCP/IP depending on the revision of the inet package installed on your system. To check its version execute:

    pkginfo -x inet

For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.08)
For inet 6.01.xx.xx: - Not vulnerable.
For inet 6.02.xx.xx: - Not vulnerable.

The NetBSD Project
Topic 1 - Teardrop
Versions 1.2 and above are not vulnerable.

Topic 2 - Land
Versions prior to 1.3_BETA will hang. 1.3_BETA and later versions are not vulnerable.

Red Hat Software
Topic 1 - Teardrop
Linux is not vulnerable.
Linux is not vulnerable.

Sun Microsystems, Inc.

All releases of Solaris are not vulnerable. All supported versions of SunOS 4.1.x (4.1.3_U1 and 4.1.4) are not vulnerable.

All releases of Solaris are not vulnerable. SunOS 4.1.3_U1 and 4.1.4 are vulnerable. The following patches should be installed:

<table>
<thead>
<tr>
<th>SunOS version</th>
<th>Patch Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.4</td>
<td>102517-05</td>
</tr>
<tr>
<td>4.1.3_U1</td>
<td>102010-06</td>
</tr>
</tbody>
</table>

Sun recommended and security patches (including checksums) are available from:

http://sunsolve.sun.com/sunsolve/pubpatches/patches.html

The CERT Coordination Center thanks Paul Ferguson and Daniel Senie for providing information on network ingress filtering.


Revision History

May 26, 1998  Updated vendor information for Sun Microsystems, Inc.
Apr. 28, 1998 Corrected URL for obtaining RFCs.
Jan. 29, 1998 Updated reference to the filtering document (now an RFC) in Section III.B.
Jan. 5, 1998 Updated vendor information for NetBSD.