# CERT Advisory CA-1997-19 lpr Buffer Overrun Vulnerability

Original issue date: June 25, 1997
Last revised: April 7, 1998
Added vendor information for Silicon Graphics Inc.

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

The technical content of this advisory was originally published by AUSCERT (AA-96.12), who last updated the information on June 19, 1997. We use it here with their permission.

---

There is a vulnerability in the BSD-based printing software, lpr, available on a variety of Unix platforms. This vulnerability may allow local users to gain root privileges.

Exploit information involving this vulnerability has been publicly available for some time. Recently, the CERT/CC has received reports that the vulnerability is being actively exploited.

We recommend installing a vendor patch if one is available. Until you can do so, we recommend using the wrapper 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

A vulnerability exists in the BSD-based lpr printing package found on many Unix systems.

Due to insufficient bounds checking on arguments that are supplied by users, it is possible to overwrite the internal stack space of the lpr program while it is executing. This can allow an intruder to cause lpr to execute arbitrary commands by supplying a carefully designed argument to lpr. These commands will be run with the privileges of the lpr program. When lpr is installed setuid or setgid, it may allow intruders to gain those privileges.

When lpr is setuid root, it may allow intruders to run arbitrary commands with root privileges.

For information from vendors relating to this vulnerability, please check Appendix A of this advisory. In addition to the products mentioned, be aware that platforms using the BSD-based lpr systems, in which lpr is installed setuid or setgid, may also be vulnerable.

Note also that the vulnerability described in this advisory is not present in the LPRng printing package.

## II. Impact

Local users may gain root privileges. It is necessary to have access to an account on the system to exploit this vulnerability.

## III. Solution

The lpr printing package is available on many different systems. As vendor patches are made available sites are encouraged to install them. Until vendor patches are available, we recommend applying the workaround referred to in III.B.

### A. Install vendor patches

Specific vendor information has been placed in Appendix A. If the BSD- based lpr printing software is used and your vendor is not listed in Appendix A, please contact your vendor directly.

### B. Install lpr wrapper

Until you can install a vendor patch, we encourage you install a wrapper developed by AUSCERT to help prevent lpr being exploited using this vulnerability.

The source for the wrapper, including installation instructions, can be found at

ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/overflow_wrapper.c

This wrapper replaces the lpr program and checks the length of the command line arguments which are passed to it. If an argument exceeds a certain predefined value (MAXARGLEN), the wrapper exits without executing the lpr command. The wrapper program can also be configured to syslog any failed attempts to execute lpr with arguments exceeding MAXARGLEN. For further instructions on using this wrapper, please read the comments at the top of overflow_wrapper.c.

When compiling overflow_wrapper.c for use with lpr, AUSCERT recommends defining MAXARGLEN to be 32.

The MD5 checksum for the current version of overflow_wrapper.c can be retrieved from

ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/CHECKSUM

The CHECKSUM file has been digitally signed using the AUSCERT PGP key.

---

## Appendix A - Vendor information

Below is a list of the vendors who have provided information. 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 3.0 is not vulnerable to the problem.

BSDI have issued a patch which addresses this vulnerability under BSD/OS 2.1. This patch is available from:

ftp://ftp.bsdi.com/pub/bsdi/patches/patches-2.1/U210-028

## Digital Equipment Corporation

Digital Equipment Corporation
Software Security Response Team
Copyright (c) Digital Equipment Corporation 1997. All rights reserved.

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

- DIGITAL EQUIPMENT CORPORATION 06/19/97

## FreeBSD

This problem was fixed prior to the release of FreeBSD 2.1.6 and 2.2. Users running older versions of the OS should review the security advisory describing this vulnerability (SA-96.18) at:

ftp://freebsd.org/pub/CERT/advisories/FreeBSD-SA-96:18.lpr.asc

Patches can be found in the directory:

ftp://freebsd.org/pub/CERT/patches/SA-96:18

## IBM Corporation

AIX is not vulnerable to the lpr buffer overflow. The version of lpr shipped with AIX is not installed with the setuid bit turned on.

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

## Linux

The Linux Emergency Response Team have released a Linux Security FAQ Update which addresses this vulnerability. This Update contains information regarding various Linux distributions.

It is available from:

ftp://bach.cis.temple.edu/pub/Linux/Security/FAQ/updates/Update-11-25-1996.vulnerability-lpr-0.06-v1.2

## NCR Corporation

The lpr command is not installed as a set-uid command on NCR MP-RAS Unix SVR4 systems, which means MP-RAS is not vulnerable.

## NEXT

The NEXT group has addressed the vulnerability described in this advisory in release 4.2 of OpenStep/Mach.

## The Santa Cruz Operation, Inc. (SCO)

SCO has determined that the following SCO operating systems are not vulnerable:

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

## Silicon Graphics Inc.

For patch information, see Silicon Graphics Inc. Security Advisory, Number 19980402-01-PX, "lp(1) Security Vulnerabilities," available from:

ftp://sgigate.sgi.com/security/19980402-01-PX

## Sun Microsystems, Inc.

All versions of Solaris are not affected. SunOS 4.1.3_U1 and SunOS 4.1.4 are vulnerable. Sun recommends that sites using SunOS 4.1.3_U1 and SunOS 4.1.4 apply the workaround provided in this advisory.

---

The CERT Coordination Center staff thanks AUSCERT for permission to republish the information in their advisory AA-96.12. AUSCERT originally thanked Alexander O. Yuriev, the FreeBSD security team, IBM, and the CERT/CC for their assistance in the production of their advisory.

---

Revision History

| | |
|---|---|
| Apr.  7, 1998 | Added vendor information for Silicon Graphics Inc. |
| Dec.  5, 1997 | Added vendor information for NCR Corporation. |
| Sep. 30, 1997 | Updated copyright statement |