

[Full-Disclosure] NetBSD Security Advisory 2003-003 Buffer Overflow in file(1)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-03/0105.html>

From: NetBSD Security Officer (security-officer@netbsd.org)

Date: 03/12/03

From: NetBSD Security Officer <security-officer@netbsd.org>

To: full-disclosure@lists.netsys.com

Date: Wed, 12 Mar 2003 11:59:24 -0500

-----BEGIN PGP SIGNED MESSAGE-----

NetBSD Security Advisory 2003-003

=====

Topic: Buffer Overflow in file(1)

Version: NetBSD-current: source prior to February 27, 2003

NetBSD 1.6: affected

NetBSD-1.5.3: affected

NetBSD-1.5.2: affected

NetBSD-1.5.1: affected

NetBSD-1.5: affected

Severity: Inducing a user to run file(1) could execute code as the user

Fixed: NetBSD-current: February 26, 2003

NetBSD-1.6 branch: March 8, 2003 (1.6.1 includes the fix)

NetBSD-1.5 branch: March 9, 2003 (1.5.4 includes the fix)

Abstract

=====

If file(1) is run over a specially constructed ELF file, an exploitable stack overflow occurs and attackers can gain the privileges of the user running file(1).

Technical Details

=====

A buffer overflow has been found in the file(1) program. If a user were to run file(1) over a specially doctored ELF file, arbitrary code would be executed as a result. Thus, if an attacker can somehow induce

Full-Disclosure: [Full-Disclosure] NetBSD Security Advisory 2003-003 Buffer Overflow in file(1)

a user to run file(1) over a file the attacker controls, the attacker may gain any system privileges the victim possesses.

See iDEFENSE Security Advisory 03.04.03
<http://www.idefense.com/advisory/03.04.03.txt>

Solutions and Workarounds

=====

The following instructions describe how to upgrade your file(1) binaries by updating your source tree and rebuilding and installing a new version of file(1).

* NetBSD-current:

Systems running NetBSD-current dated from before 2003-02-27 should be upgraded to NetBSD-current dated 2003-02-27 or later.

The following files need to be updated from the netbsd-current CVS branch (aka HEAD) to the respective revisions:

```
src/usr.bin/file/readelf.c: 1.17
src/usr.bin/file/softmagic.c: 1.31
```

To update from CVS, re-build, and re-install file:

```
# cd src
# cvs update -d -A -P usr.bin/file
# cd usr.bin/file

# make cleandir dependall
# make install
```

* NetBSD 1.6:

The binary distribution of NetBSD 1.6 is vulnerable.

Systems running NetBSD 1.6 sources dated from before 2003-03-09 should be upgraded from NetBSD 1.6 sources dated 2003-03-09 or later.

NetBSD 1.6.1 will include the fix.

The following files need to be updated from the netbsd-1-6 CVS branch to the respective revisions:

```
src/usr.bin/file/readelf.c: 1.13.2.1
src/usr.bin/file/softmagic.c: 1.26.2.1
```

To update from CVS, re-build, and re-install file:

```
# cd src
# cvs update -d -r netbsd-1-6 -P usr.bin/file
# cd usr.bin/file
```

Full-Disclosure: [Full-Disclosure] NetBSD Security Advisory 2003-003 Buffer Overflow in file(1)

```
# make cleandir dependall
# make install
```

* NetBSD 1.5, 1.5.1, 1.5.2, 1.5.3:

The binary distribution of NetBSD 1.5.3 is vulnerable.

Systems running NetBSD 1.5, 1.5.1, 1.5.2, or 1.5.3 sources dated from before 2003-03-10 should be upgraded from NetBSD 1.5.* sources dated 2003-03-10 or later.

The following files need to be updated from the netbsd-1-5 CVS branch to the respective revisions:

```
src/usr.bin/file/readelf.c: 1.6.4.3
src/usr.bin/file/softmagic.c: 1.18.4.2
```

To update from CVS, re-build, and re-install file:

```
# cd src
# cvs update -d -r netbsd-1-5 -P usr.bin/file
# cd usr.bin/file
```

```
# make cleandir dependall
# make install
```

Thanks To

=====

Lubomir Sedlacik and Antti Kantee, for drawing our attention to the problem.

Christos Zoulas, for aiding in the solution and with this advisory.

Revision History

=====

2003-03-12 Initial release

More Information

=====

Advisories may be updated as new information becomes available.

The most recent version of this advisory (PGP signed) can be found at

<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-003.txt.asc>

Information about NetBSD and NetBSD security can be found at

<http://www.NetBSD.ORG/> and <http://www.NetBSD.ORG/Security/>.

Copyright 2003, The NetBSD Foundation, Inc. All Rights Reserved.

Redistribution permitted only in full, unmodified form.

\$NetBSD: NetBSD-SA2003-003.txt,v 1.7 2003/03/12 03:51:31 david Exp \$

Full-Disclosure: [Full-Disclosure] NetBSD Security Advisory 2003-003 Buffer Overflow in file(1)

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.6 (NetBSD)

Comment: For info see <http://www.gnupg.org>

iQCVAwUBPm9Mmz5Ru2/4N2IFAQEi1gQAkTTyWWzv+w4E+A+K0cpiAtmqoDv9I7B6
WmIy/o9U5/uvvI1JpOK3/QKI/QKsXQ1OC2/yK63nTv3rwb+m5olywGkE7DY4ObQk
9SnBe+lsVQbjTEM/IBCmwy86h9xTmiP4xrtF8Mw/rGN0HLOWHUIxkvOn+zYWH1jd
gS5Tn2BNd2c=
=urmE

-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>