

FreeBSD Security Advisory

FreeBSD-SA-03:09.signal [REVISED]

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-08/0166.html>

From: FreeBSD Security Advisories (*security-advisories_at_freebsd.org*)

Date: 08/13/03

Date: Tue, 12 Aug 2003 15:37:48 -0700 (PDT)

To: FreeBSD Security Advisories <security-advisories@freebsd.org>

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

Hash: SHA1

FreeBSD-SA-03:09.signal Security Advisory
The FreeBSD Project

Topic: Insufficient range checking of signal numbers

Category: core

Module: sys

Announced: 2003-08-10

Affects: All releases of FreeBSD up to and including 4.8-RELEASE-p1,
5.1-RELEASE (but see `Impact' below)

FreeBSD 4-STABLE prior to the correction date

Corrected: 2003-08-10 23:09:28 UTC (RELENG_4)

2003-08-10 23:14:08 UTC (RELENG_5_1)

2003-08-10 23:17:48 UTC (RELENG_5_0)

2003-08-10 23:19:35 UTC (RELENG_4_8)

2003-08-11 10:14:38 UTC (RELENG_4_7)

2003-08-11 10:16:35 UTC (RELENG_4_6)

2003-08-12 20:23:24 UTC (RELENG_4_5)

2003-08-12 20:23:51 UTC (RELENG_4_4)

2003-08-12 20:24:13 UTC (RELENG_4_3)

FreeBSD only: YES

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit

<URL:<http://www.freebsd.org/security/>>.

0. Revision History

v1.0 2003-08-10 Initial release

v1.1 2003-08-11 Updated correction details for RELENG_4_7,

RELENG_4_6, RELENG_4_5, RELENG_4_4, RELENG_4_3
branches. Corrected an internal section reference.
Corrected a source file path name.

I. Background

Signals are a UNIX mechanism for handling asynchronous events such as pressing the terminal interrupt key (e.g. Ctrl–C), job control, memory access violations, I/O completion, and many others. Each signal is assigned a positive number. There are a number of mechanisms by which a process may cause a signal to be sent, including using the kill(2) system call or registering with certain device drivers.

II. Problem Description

Some mechanisms for causing a signal to be sent did not properly validate the signal number, in some cases allowing the kernel to attempt to deliver a negative or out–of–range signal number. Such errors were present in the ptrace(2) system call and the `spigot' video capture device driver.

The error in ptrace(2) was introduced in FreeBSD version 4.2–RELEASE (4–STABLE dated Oct 26 04:34:41 2000 UTC).

The `spigot' device driver (including the error) was introduced in FreeBSD 2.0.5. It has never been included in the kernel installed by default, nor in the GENERIC kernel configuration. Only systems with `device spigot' added to the kernel configuration are affected by this instance of the error.

III. Impact

In most cases, attempted delivery of a negative or out–of–range signal number will trigger an assertion failure and panic, thereby crashing the system. A malicious local user could use this vulnerability as a local denial–of–service attack.

However, in FreeBSD 5.x, the assertion code is not present if the `INVARIANTS' kernel option is not used. In FreeBSD 5.0–RELEASE and 5.1–RELEASE, `INVARIANTS' is not enabled by default. In this configuration, a malicious local user could use this vulnerability to modify kernel memory, potentially leading to complete system compromise. (FreeBSD 4.x is not vulnerable in this way.)

IV. Workaround

There is no workaround for the local denial–of–service attack.

The more severe impact, present only in FreeBSD 5.x systems, can be avoided by uncommenting or adding the `INVARIANTS' line to your kernel configuration:

```
options INVARIANTS #Enable calls of extra sanity checking
```

Recompile your kernel as described in
<URL:<http://www.freebsd.org/handbook/kernelconfig.html>>
and reboot the system.

NOTE WELL: This workaround is only for FreeBSD 5.x systems. This
workaround does not eliminate the possibility of a local
denial-of-service attack.

V. Solution

1) Upgrade your vulnerable system to 4.8–STABLE, or to any of the
RELENG_4_8 (4.8–RELEASE–p2), RELENG_4_7 (4.7–RELEASE–p12), or
RELENG_5_1 (5.1–RELEASE–p1) security branches dated after the
respective correction dates.

2) To patch your present system:

a) Download the relevant patch from the location below, and verify the
detached PGP signature using your PGP utility.

```
[FreeBSD 5.1–RELEASE]
```

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal51.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal51.patch.asc
```

```
[FreeBSD 5.0–RELEASE]
```

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal50.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal50.patch.asc
```

```
[FreeBSD 4.8–RELEASE, 4.8–STABLE, 4.7–STABLE dated Jan 2 20:39:13 2003 UTC  
or later]
```

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal4s.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal4s.patch.asc
```

```
[FreeBSD 4.3–RELEASE through 4.7–RELEASE, 4.7–STABLE dated before  
Jan 2 20:39:13 2003 UTC]
```

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal47.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal47.patch.asc
```

b) Apply the patch.

```
# cd /usr/src  
# patch < /path/to/patch
```

c) Recompile your kernel as described in
<URL:<http://www.freebsd.org/handbook/kernelconfig.html>>

and reboot the system.

VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

Branch Revision

Path

```
src/sys/UPDATING
  RELENG_5_1 1.251.2.2
  RELENG_5_0 1.229.2.15
  RELENG_4_8 1.73.2.80.2.4
  RELENG_4_7 1.73.2.74.2.15
  RELENG_4_6 1.73.2.68.2.43
  RELENG_4_5 1.73.2.50.2.45
  RELENG_4_4 1.73.2.43.2.46
  RELENG_4_3 1.73.2.28.2.33
src/sys/conf/newvers.sh
  RELENG_5_1 1.50.2.3
  RELENG_5_0 1.48.2.10
  RELENG_4_8 1.44.2.29.2.3
  RELENG_4_7 1.44.2.26.2.14
  RELENG_4_6 1.44.2.23.2.32
  RELENG_4_5 1.44.2.20.2.29
  RELENG_4_4 1.44.2.17.2.37
  RELENG_4_3 1.44.2.14.2.23
src/sys/i386/isa/spigot.c
  RELENG_4 1.44.2.1
  RELENG_5_1 1.58.2.1
  RELENG_5_0 1.55.2.1
  RELENG_4_8 1.44.14.1
  RELENG_4_7 1.44.12.1
  RELENG_4_6 1.44.10.1
  RELENG_4_5 1.44.8.1
  RELENG_4_4 1.44.6.1
  RELENG_4_3 1.44.4.1
src/sys/kern/sys_process.c
  RELENG_4 1.51.2.7
  RELENG_5_1 1.108.2.1
  RELENG_5_0 1.104.2.1
  RELENG_4_8 1.51.2.6.2.1
  RELENG_4_7 1.51.2.4.2.2
  RELENG_4_6 1.51.2.3.4.2
  RELENG_4_5 1.51.2.3.2.2
  RELENG_4_4 1.51.2.1.4.3
  RELENG_4_3 1.51.2.1.2.3
src/sys/kern/kern_sig.c
  RELENG_5_1 1.239.2.1
  RELENG_5_0 1.197.2.1
```

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

Version: GnuPG v1.2.2 (FreeBSD)

iD8DBQE/OVDMFdaIBMps37IRAsaBAJ4zAzw4sDcu2oc/M7iiXfLQzg8WogCeNqeF
Di+jeJfFrpGAh+/JxUAW/60=
=qXMR

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

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"