-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

```
================================================================================
FreeBSD-SA-26:16.libnv                                        Security Advisory
                                                            The FreeBSD Project

Topic:          Stack overflow via select() file descriptor set overflow

Category:       core
Module:         libnv
Announced:      2026-04-29
Credits:        Joshua Rogers of AISLE Research Team
Affects:        All supported versions of FreeBSD.
Corrected:      2026-04-29 14:47:51 UTC (stable/15, 15.0-STABLE)
                2026-04-29 14:48:32 UTC (releng/15.0, 15.0-RELEASE-p7)
                2026-04-29 14:48:56 UTC (stable/14, 14.4-STABLE)
                2026-04-29 14:49:47 UTC (releng/14.4, 14.4-RELEASE-p3)
                2026-04-29 14:49:27 UTC (releng/14.3, 14.3-RELEASE-p12)
                2026-04-29 14:50:09 UTC (stable/13, 13.5-STABLE)
                2026-04-29 14:50:21 UTC (releng/13.5, 13.5-RELEASE-p13)
CVE Name:       CVE-2026-39457

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit <URL:https://security.FreeBSD.org/>.

I.   Background

libnv is a general-purpose library designed for storing and exchanging sets
of name-value pairs.  This library can serve as an Inter-Process
Communication (IPC) framework, enabling processes to exchange data and file
descriptors.  For example, it is used in libcasper to establish communication
between privileged and unprivileged processes.  Additionally, libnv can
function as an interface for communication between userland and kernel.

Originally, libnv was inspired by OpenZFS' nvlist implementation.  However,
the implementations are separate.  This advisory relates only to the base
system implementation of libnv, not to the one in OpenZFS.

II.  Problem Description

When exchanging data over a socket, libnv uses select(2) to wait for data to
arrive.  However, it does not verify whether the provided socket descriptor
fits in select(2)'s file descriptor set size limit of FD_SETSIZE (1024).

III. Impact

An attacker who is able to force a libnv application to allocate large file
descriptors, e.g., by opening many descriptors and executing a program which
is not careful to close them upon startup, can trigger stack corruption.  If
the target application is setuid-root, then this could be used to elevate
local privileges.

IV.  Workaround

No workaround is available.

V.   Solution

Upgrade your vulnerable system to a supported FreeBSD stable or
release / security branch (releng) dated after the correction date
and reboot.
```

Perform one of the following:

1) To update your vulnerable system via a binary patch:

Systems running a RELEASE version of FreeBSD on the amd64 or arm64 platforms, or the i386 platform on FreeBSD 13, can be updated via the freebsd-update(8) utility:

```
# freebsd-update fetch
# freebsd-update install
# shutdown -r +10min "Rebooting for a security update"
```

2) To update your vulnerable system via a source code patch:

The following patches have been verified to apply to the applicable FreeBSD release branches.

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

```
# fetch https://security.FreeBSD.org/patches/SA-26:16/libnv.patch
# fetch https://security.FreeBSD.org/patches/SA-26:16/libnv.patch.asc
# gpg --verify libnv.patch.asc
```

b) Apply the patch. Execute the following commands as root:

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

c) Recompile the operating system using buildworld and installworld as described in <URL:https://www.FreeBSD.org/handbook/makeworld.html>.

d) Recompile your kernel as described in <URL:https://www.FreeBSD.org/handbook/kernelconfig.html> and reboot the system.

VI. Correction details

This issue is corrected as of the corresponding Git commit hash in the following stable and release branches:

Branch/path	Hash	Revision
stable/15/	025789eaa648	stable/15-n283380
releng/15.0/	7e4d5363ddce	releng/15.0-n281032
stable/14/	45809b0e1bc1	stable/14-n274081
releng/14.4/	a5cb4863d65a	releng/14.4-n273696
releng/14.3/	a872c32f389e	releng/14.3-n271496
stable/13/	4acc2b5c61a7	stable/13-n259862
releng/13.5/	32d12677ff45	releng/13.5-n259218

Run the following command to see which files were modified by a particular commit:

```
# git show --stat <commit hash>
```

Or visit the following URL, replacing NNNNNN with the hash:

<URL:https://cgit.freebsd.org/src/commit/?id=NNNNNN>

To determine the commit count in a working tree (for comparison against nNNNNNN in the table above), run:

```
# git rev-list --count --first-parent HEAD
```

VII. References

<URL:https://www.cve.org/CVERecord?id=CVE-2026-39457>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:16.libnv.asc>

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

iQJPBAEBCgA5FiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnySTUbFIAAAAAABAAO
bWFudTIsMi41KzEuMTIsMCwzAAoJEG5Y3pAfABrvEdwQAKF0kwMDT0ZjvcDnvqXa
NmJEse7XRdFDWDcMp8NtSQK5DTYBRpUgwWiC7M+HRr4QIf/aIjzwuJdu1luK913i
vAJJUbAaEAdGbNqd35FtDlnTWQE638R4HQ0TqMBrUfGTSp0O5SPOpTSPXB1Fw/F7
Q3c22lNDHgxgZ8+DOoJH70HgjdVskz3ezZroYUKfmk5vh9yZtVM9zMr6iGr6TUA7
OEbIrMlRCJ3pI9dOSGNKz1i/3s8bMS3U3nvAWIYPdSjKQBOyRdHoZHtk4SfY9TVs
epqQQccUv9g5+E1QgxxoQHLR4dLkCHEJKOU2sqc/qW9KISX2rsTd2UYgYubxtb+j
CIzTg23/rkMMhCi3VZ9NVLmGrxZclxyvAVJ/V3942jjag0c1onc+5RH0IGAljgay
hobn3CBqE2NIOjoFyCJK9RcZ+wtvxFoQFdX6A56h5vDD2I/H7MIFJ0EnW3aWvT8f
0xiWhD4//9AU3+06soPt6l4tE/YaXJbcvYb92kC1JbbGVApMrDYbdxu3QK8HwAlV
mNTFd3hgoEzlCiFH9vDNK/RIsVE67kb4KjqZKC1ElWrQbawQZtnKUigpxGcZbhCC
9zwXgoFRHCzeBiO77anQMgArNuY3Wj29beepzCvOA7u/KRyDTvDat8YRWNKbWS5L
T3cMyFqgRkUgr7tajk0L51Xx
=Edvm
-----END PGP SIGNATURE-----