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

```
================================================================================
FreeBSD-SA-26:17.libnv                                        Security Advisory
                                                            The FreeBSD Project

Topic:          Heap overflow in libnv

Category:       core
Module:         libnv
Announced:      2026-04-29
Credits:        Mariusz Zaborski
Affects:        All supported versions of FreeBSD.
Corrected:      2026-04-29 14:47:52 UTC (stable/15, 15.0-STABLE)
                2026-04-29 14:48:33 UTC (releng/15.0, 15.0-RELEASE-p7)
                2026-04-29 14:48:57 UTC (stable/14, 14.4-STABLE)
                2026-04-29 14:49:48 UTC (releng/14.4, 14.4-RELEASE-p3)
                2026-04-29 14:49:28 UTC (releng/14.3, 14.3-RELEASE-p12)
                2026-04-29 14:50:10 UTC (stable/13, 13.5-STABLE)
                2026-04-29 14:50:22 UTC (releng/13.5, 13.5-RELEASE-p13)
CVE Name:       CVE-2026-35547

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 the one in OpenZFS.

II.  Problem Description

When processing the header of an incoming message, libnv failed to properly
validate the message size.

III. Impact

The lack of validation allows a malicious program to write outside the bounds
of a heap allocation.  This can trigger a crash or system panic, and it may
be possible for an unprivileged user to exploit the bug to elevate their
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.

Perform one of the following:

1) To update your vulnerable system installed from base system packages:
```

Systems running a 15.0-RELEASE version of FreeBSD on the amd64 or arm64
platforms, which were installed using base system packages, can be updated
via the pkg(8) utility:

```
# pkg upgrade -r FreeBSD-base
# shutdown -r +10min "Rebooting for a security update"
```

2) To update your vulnerable system installed from binary distribution sets:

Systems running a RELEASE version of FreeBSD on the amd64 or arm64 platforms,
or the i386 platform on FreeBSD 13, which were not installed using base
system packages, can be updated via the freebsd-update(8) utility:

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

3) 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-26:17/libnv.patch
# fetch https://security.FreeBSD.org/patches/SA-26:17/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 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/	414e25d7d512	stable/15-n283381
releng/15.0/	b345e07c8d71	releng/15.0-n281033
stable/14/	1cbd6e148249	stable/14-n274082
releng/14.4/	4f0992ce23b0	releng/14.4-n273697
releng/14.3/	aa15809f85de	releng/14.3-n271497
stable/13/	05b91c2a7106	stable/13-n259863
releng/13.5/	f7f48005fbe2	releng/13.5-n259219

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-2026-35547>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:17.libnv.asc>

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

iQJPBAEBCgA5FiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnySTgbFIAAAAAABAAO
bWFudTIsMi41KzEuMTIsMCwzAAoJEG5Y3pAfABrvV+cQANyoTjQKCgT/ObIaHIvn
/ZHiHhWtxqpnOGHiJQ/Pu32XfF4zngUmxH3RFM4V+p2QTKd+OnCojcr/nWjS1Xh4
D2G0TUYeTfEUzERLxODtWSxD6Px0n7qutRgpTx9yLid3N34av93aoQYnK+1FkqAf
PonQlVKqI2Ab44879/Aw4glrjNQg2kGzAwSA4Nzik96BZMePQk6sDnzNKODz914O
khZ6KDSc9Fc0jUS4RZUh1AXnAEV2a7vD3fQLg+8aegFiaIajnC4dFZPjl1jioawp
0Jm0f1UI/n5jfp/zyHCJZIgDNvcX+laFnLRJuB8XCrWk8luFdpVOTUjsuPMSA737
TwdSG05ZnGhWsJhQjK0mdkDxoH81wWW7mz21jjVBJ9UhaWhGMNV4mBSevfFYkFkb
JHuHO0aCUB6e6/MJ/7O6d0tG9etdQUjCpQeLqXKiYQKqjQkplUUL0C2Uy7A4otEu
MelMjHsQMQEjUpRVxX4IADyNQgtJjrroFDdoez3oBF1dfBxQrKkWBnKTTYrV6cbl
fIVmkl2b6B/0FcGhAekDh1tLvHj4Ul0n8wzb19F7vT1+4QlnLOtIrXZcJdsTbqde
tKRoUYcwvBpUn2bsefxWzEPZ9jvSBoIkSwPmSnu8zQ1jY44eyiHodaXkMsZygplL
WfRkGmyutQ0XdUuhcCSyfi/G
=K9xn
-----END PGP SIGNATURE-----