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

```
================================================================================
FreeBSD-SA-26:10.tty                                        Security Advisory
                                                          The FreeBSD Project

Topic:          Kernel use-after-free bug in the TIOCNOTTY handler

Category:       core
Module:         tty
Announced:      2026-04-21
Credits:        Nicholas Carlini using Claude, Anthropic
Affects:        All supported versions of FreeBSD.
Corrected:      2026-04-21 15:43:02 UTC (stable/15, 15.0-STABLE)
                2026-04-21 15:44:27 UTC (releng/15.0, 15.0-RELEASE-p6)
                2026-04-21 15:43:13 UTC (stable/14, 14.4-STABLE)
                2026-04-21 15:45:31 UTC (releng/14.4, 14.4-RELEASE-p2)
                2026-04-21 15:46:01 UTC (releng/14.3, 14.3-RELEASE-p11)
                2026-04-21 15:43:56 UTC (stable/13, 13.5-STABLE)
                2026-04-21 15:47:07 UTC (releng/13.5, 13.5-RELEASE-p12)
CVE Name:       CVE-2026-5398

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

TIOCNOTTY is an ioctl(2) operation which allows a process to detach itself
from its controlling terminal.  Unprivileged processes may use this ioctl.
See the tty(4) manual page for more information on its usage.

II.  Problem Description

The implementation of TIOCNOTTY failed to clear a back-pointer from the
structure representing the controlling terminal to the calling process'
session.  If the invoking process then exits, the terminal structure
may end up containing a pointer to freed memory.

III. Impact

A malicious process can abuse the dangling pointer to grant itself root
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 the system.

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.

[FreeBSD 15.0]
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-15.patch
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-15.patch.asc
# gpg --verify tty-15.patch.asc

[FreeBSD 14.4]
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-14.4.patch
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-14.4.patch.asc
# gpg --verify tty-14.4.patch.asc

[FreeBSD 14.3]
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-14.3.patch
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-14.3.patch.asc
# gpg --verify tty-14.3.patch.asc

[FreeBSD 13.5]
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-13.patch
# fetch https://security.FreeBSD.org/patches/SA-26:10/tty-13.patch.asc
# gpg --verify tty-13.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/                              0c6b1e0864b8    stable/15-n283065
releng/15.0/                            fdee312d0c97  releng/15.0-n281022
stable/14/                              f46210a7ab32    stable/14-n273997
releng/14.4/                            af294329c57f  releng/14.4-n273685
releng/14.3/                            44077c07f19f  releng/14.3-n271485
stable/13/                              5eae7f23fe0e    stable/13-n259845
releng/13.5/                            2862a33bdd1c  releng/13.5-n259210
- -------------------------------------------------------------------------
```

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-2026-5398>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:10.tty.asc>
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnnoaMACgkQbljekB8A
Gu8qzA//fuGHRB8Y+n+EUyAGycr0PGMeG423hykkYBAvfBJJP5RYv4Ter79YAeuu
zqXqijjr+yyKcE1+km63/koxUXZmkbpR2Xt/0i2d3jAqnrUioZqwc+llCgqhh6Dr
AhyDn+xCtCWJow0Iktlk6ZHEuQLX6kwGxT/1cvmcnhZE8XQf2PNEbRk8oit+kf8c
LQZF2EBK4wPh5Lik8DvqoyX1k7B44jVhL2AMqs/2fRdTFluY/MIgvbRsRdCQRLJE
doXA2YdDljkTJpAPIg31WP6C7L0LPkeyRm4Xn3zBt4SalyiChfQ9kQYcdQS7/lt4
LUyrQKQHVtVx2SseYFTtPoncYl2IEmaHOAZkQrfzxFybYryoq4macGbuNZh0Aygq
mpIAIIDKAyKQCcDGzluRL4ksoPyw9Kav7SJJ83P9khrKINaNg5NZc1Ptc7K/UvSk
H5XKwHBaURcXGzl1crBtqbbK5lEvO/UaxXraMwqCTM+WqF7dND2KvSbZEma/FJ8l
7Wcszs2dvgC2dQghlmRlxxYvMGzf49XO4+Y64WarMqmLTAyDV9nBrZGMUj1M2nqC
rgylEscbOn8z/Yq8vpr0sydYRVDBHtVMOaztsqFylGnzRfSjQQH3yuJ40ngvy9yo
GexBhYXFyrruuuuz9p9xplIRzVkHVjkrm9/zwe4bSBylQ+/MeGQ=
=crMa
-----END PGP SIGNATURE-----