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

```
================================================================================
FreeBSD-SA-25:09.netinet                                        Security Advisory
                                                              The FreeBSD Project

Topic:          SO_REUSEPORT_LB breaks connect(2) for UDP sockets

Category:       core
Module:         netinet
Announced:      2025-10-22
Credits:        MSc. student Omer Ben Simhon and Prof. Amit Klein,
                both from the Hebrew University School of Computer
                Science and Engineering
Affects:        All supported versions of FreeBSD.
Corrected:      2025-10-22 15:48:25 UTC (stable/15, 15.0-STABLE)
                2025-10-22 15:50:30 UTC (releng/15.0, 15.0-BETA2-p1)
                2025-10-22 15:48:51 UTC (stable/14, 14.3-STABLE)
                2025-10-22 15:51:57 UTC (releng/14.3, 14.3-RELEASE-p5)
                2025-10-22 15:49:32 UTC (stable/13, 13.4-STABLE)
                2025-10-22 15:53:35 UTC (releng/13.5, 13.5-RELEASE-p6)
CVE Name:       CVE-2025-24934

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

SO_REUSEPORT_LB is a socket option, set by setsockopt(2), which allows multiple
TCP or UDP sockets to bind to the same socket address, creating a
load-balancing group.  Incoming packets and connections are distributed evenly
among sockets in a group.  This helps network services avoid scalability
bottlenecks caused by having a single TCP listening socket.  In particular, it
is expected that sockets belonging to a load-balancing group will accept
packets from any source address.

II.  Problem Description

Connected sockets are not intended to belong to load-balancing groups.
However, the kernel failed to check the connection state of sockets when adding
them to load-balancing groups.  Furthermore, when looking up the destination
socket for an incoming packet, the kernel will match a socket belonging to a
load-balancing group even if it is connected.

Connected sockets are only supposed to receive packets originating from the
connected host.  The above behavior violates this contract.

III. Impact

Software which sets SO_REUSEPORT_LB on a socket and then connects it to a host
will not observe any problems.  However, due to its membership in a
load-balancing group, that socket will receive packets originating from any
host.  This breaks the contract of the connect(2) and implied connect via
sendto(2), and may leave the application vulnerable to spoofing attacks.

IV.  Workaround

No workaround is available.  Software which does not use SO_REUSEPORT_LB is
not affected.

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 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.

```
[FreeBSD 15.x]
# fetch https://security.FreeBSD.org/patches/SA-25:09/netinet-15.patch
# fetch https://security.FreeBSD.org/patches/SA-25:09/netinet-15.patch.asc
# gpg --verify netinet-15.patch.asc

[FreeBSD 14.x]
# fetch https://security.FreeBSD.org/patches/SA-25:09/netinet-14.patch
# fetch https://security.FreeBSD.org/patches/SA-25:09/netinet-14.patch.asc
# gpg --verify netinet-14.patch.asc

[FreeBSD 13.x]
# fetch https://security.FreeBSD.org/patches/SA-25:09/netinet-13.patch
# fetch https://security.FreeBSD.org/patches/SA-25:09/netinet-13.patch.asc
# gpg --verify netinet-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/	ef159100ec2b	stable/15-n280782
releng/15.0/	98c539667881	releng/15.0-n280723
stable/14/	e276759b3687	stable/14-n272700
releng/14.3/	058bcb57cd4b	releng/14.3-n271448
stable/13/	df888c8f41f6	stable/13-n259508
releng/13.5/	90e14aa082d3	releng/13.5-n259180

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-24934>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-25:09.netinet.asc>
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEthUnfoEIffdcgYM7bljekB8AGu8FAmj5CrEACgkQbljekB8A
Gu98YQ//dMMpEdKapK6bBM++8HoSWeydnoUifFqu3LiDXcDTgQ6jVsmwQ/QOUPll
bOB7etdtu+FQEI4yl8d9w98TrXC8Mvl6p+dZ3SkIglLNeVmouiot+VDBpoOr/EPq
xXf6dGlkDneYTsAFXwDKe48vmisdWd1trtYhVuE6qWq54AH4Y3dv0+DOMIdlKbPc
GHFLRoJ/eEJH+3QAhL8Ozdp2WySUWHPMsScBRldcrhariXzEQ9KcM6TJx8mYGKta
DYeezna1DQ87wU8Zs5fKfhUS6q/YJcXr9Te5P1xirmcmgr2frJW1DjfWKI8oQ9ru
2mn6oedSu6nRFjpYzO9tS/7svC8Hkyyr1rsZujRkC5cMRwY2DovU653GoaOwadMc
gig8CvOeb1srD1kMnFyGfa54VTbGZCZ261bnGdUc9BCL8ARtv6q4KNTRofkYrCLP
YwGTxEsCVdNbtDGv5nLJ/V7RfAUMnp9YuYpHc0Auttt6cUW6DI3nGQg+LlfoCJ0n
JESXa3Fry0GcFWiPB6oigyFSH6c3Ml+E7TiUYAZOtQ4cqJG1v9x1Lv5BQ1dz5vah
J24oGW2uI6Xp0TbvIFBd6KCFZSa/dS9sq486norj17X7ktZ7EeVVpm4vRBtDEo4N
k2WdkjcWfSM5uLnYLZR+rp+1rhtSIxw3gZaoJLl18p+9NMOFBH4=
=RgID
-----END PGP SIGNATURE-----
```