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

================================================================================
FreeBSD-SA-26:09.pf                                          Security Advisory
                                                          The FreeBSD Project

Topic:          pf silently ignores certain rules

Category:       core
Module:         pf
Announced:      2026-03-25
Credits:        Michael Gmelin
Affects:        FreeBSD 14.x and FreeBSD 15.0
Corrected:      2026-03-25 07:11:58 UTC (stable/15, 15.0-STABLE)
                2026-03-26 01:11:25 UTC (releng/15.0, 15.0-RELEASE-p5)
                2026-03-25 09:58:28 UTC (stable/14, 14.4-STABLE)
                2026-03-26 01:15:00 UTC (releng/14.4, 14.4-RELEASE-p1)
                2026-03-26 01:16:06 UTC (releng/14.3, 14.3-RELEASE-p10)
CVE Name:       CVE-2026-4748

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

pf is an Internet Protocol packet filter originally written for OpenBSD.
While loading its configuration, pf hashes rules and silently drops
duplicates as an optimisation.  Only the first rule with the same hash is
considered.

II.  Problem Description

A regression in the way hashes were calculated caused rules containing the
address range syntax (x.x.x.x - y.y.y.y) that only differ in the address
range(s) involved to be silently dropped as duplicates.  Only the first of
such rules is actually loaded into pf.  Ranges expressed using the
address[/mask-bits] syntax were not affected.

Some keywords representing actions taken on a packet-matching rule, such as
'log', 'return tll', or 'dnpipe', may suffer from the same issue.  It is
unlikely that users have such configurations, as these rules would always be
redundant.  The verification described in "IV. Workaround" below will find
these as well.

III. Impact

Affected rules are silently ignored, which can lead to unexpected behaviour
including over- and underblocking.

IV.  Workaround

Only systems using the pf firewall are affected.

The operator can determine if a specific system is affected by reloading the
configuration verbosely:

# pfctl -vf /etc/pf.conf | grep already

As a workaround, affected rules can be rewritten, e.g., by
using tables or multiple rules instead of address ranges.
Another option is to add labels to rules to make them unique.
```

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 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-26:09/pf-15.patch
# fetch https://security.FreeBSD.org/patches/SA-26:09/pf-15.patch.asc
# gpg --verify pf-15.patch.asc

[FreeBSD 14.x]
# fetch https://security.FreeBSD.org/patches/SA-26:09/pf-14.patch
# fetch https://security.FreeBSD.org/patches/SA-26:09/pf-14.patch.asc
# gpg --verify pf-14.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/	4311217a039c	stable/15-n282698
releng/15.0/	d91cf52e31ac	releng/15.0-n281017
stable/14/	e3b801edded9	stable/14-n273835
releng/14.4/	b6865bca4ba5	releng/14.4-n273681

```
releng/14.3/                              c03577d99d2d  releng/14.3-n271481
- -------------------------------------------------------------------------
```

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-2026-4748>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:09.pf.asc>


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

iQIzBAEBCgAdFiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnEp+AACgkQbljekB8A
Gu84/Q//cIBdAEmzD04kjglaG1X75rULWJ0fsD26RW89Y3IEvLnUa5yoWV0dKUeW
wRta0n7cvpkLiuDVqSfasVrkVM0EZ70toWcd0JXTRwaJ+i7IhHMByXjvSwTzhS/d
OL2uDzjJ1nUyUqangNM+99Mpr3UQOEIMY9Scq5E0NNr/x6NdWXN4psiB/RCSFU64
abRos56CPkWbfVQLVZ3i2FihGhYQ2JLnqvP9DgCT6xy6MU5uTDWF57sxe4ciYWGw
4ZRydr/oyTkpthetm9xPFoFkaBiOiGfdTnsOi58f7mcWln+AgiKLzT0KdOd6XkEy
RH22v4254P4nquDXfBTIJUVyDFd8SVIk7Ol78BzRNdEYOEog6KEI3fTjArFMIiy6
CLPS92ph3xq4aBWMdxnZ4cvfW7Ktm8Zp9xrXCvdRaUGfl+wawzjfjgw62eXaec4x
pFxip2jLziZUDAvpzg1ywK0ajJE+RYh7HlT7CG2pTEcCaaIC0rJ7B2eEIaoO48Ho
Uez92JN54P7xBRLy/rLVfUHz7Td11toAg6wwBTEAQPKssDHh1DQZMLSDKZcGanlt
waUCybHeaWkMZvoHtLlEJjZ8hL/67Ivz2Huv5KCZ5CtpoEqe5ZHmGGS3iOCiuLvQ
9k2F3fkJN4w1zpGHE48JJ03FYQA7cTHwEro7TCRzeM6+KnqgAzE=
=cGmd
-----END PGP SIGNATURE-----
```