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

```
================================================================================
FreeBSD-SA-26:12.dhclient                                   Security Advisory
                                                          The FreeBSD Project

Topic:          Remote code execution via malicious DHCP options

Category:       core
Module:         dhclient
Announced:      2026-04-29
Credits:        Joshua Rogers of AISLE Research Team
Affects:        All supported versions of FreeBSD.
Corrected:      2026-04-29 14:47:47 UTC (stable/15, 15.0-STABLE)
                2026-04-29 14:48:28 UTC (releng/15.0, 15.0-RELEASE-p7)
                2026-04-29 14:48:50 UTC (stable/14, 14.4-STABLE)
                2026-04-29 14:49:41 UTC (releng/14.4, 14.4-RELEASE-p3)
                2026-04-29 14:49:22 UTC (releng/14.3, 14.3-RELEASE-p12)
                2026-04-29 14:50:06 UTC (stable/13, 13.5-STABLE)
                2026-04-29 14:50:18 UTC (releng/13.5, 13.5-RELEASE-p13)
CVE Name:       CVE-2026-42511

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

dhclient(8) is the default IPv4 DHCP client used on FreeBSD.  It is
responsible for contacting DHCP servers on a network segment and for
initialising and configuring network interfaces based on received
information.

II.  Problem Description

The BOOTP file field is written to the lease file without escaping embedded
double-quotes, allowing injection of arbitrary dhclient.conf directives.
When the lease file is subsequently re-parsed by dhclient, e.g., after a
system restart, an attacker-controlled field from the lease is passed to
dhclient-script(8), which evaluates it.

III. Impact

A rogue DHCP server may be able to execute arbirary code as root on a system
running dhclient.

IV.  Workaround

No workaround is available.  Systems not running dhclient(8) are not
affected.

The attacker needs to be on the same broadcast domain and respond to DHCP
requests.  A well-managed network will configure DHCP snooping on switches to
prevent rogue DHCP servers from operating.

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
```

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
```

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-26:12/dhclient.patch
# fetch https://security.FreeBSD.org/patches/SA-26:12/dhclient.patch.asc
# gpg --verify dhclient.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>.

Restart the applicable daemons, or 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/	2621f6c5d4ae	stable/15-n283377
releng/15.0/	e7b4fb41aafa	releng/15.0-n281029
stable/14/	b3087e05e848	stable/14-n274076
releng/14.4/	73b801e3b5b3	releng/14.4-n273691
releng/14.3/	dda71167a101	releng/14.3-n271492
stable/13/	46c01e4dd102	stable/13-n259859
releng/13.5/	a2d45189b9ee	releng/13.5-n259215

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-2026-42511>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:12.dhclient.asc>


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

iQJPBAEBCgA5FiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnySScbFIAAAAAABAAO
bWFudTIsMi41KzEuMTIsMCwzAAoJEG5Y3pAfABrv/HEQANr71RMaW0408Cp2xZ/n
DN8DsU7vCXPDcZWF/HAl+COurXipEycxnP6pBdm2uCqRGWXmNPkjyA5nyoAM2qYP
9b3rXQHKdrqc0vvbjJuahzqfttwcv1jFQp+8Z8N8TYWUnETprai5VOwZ+7p2caGC
gZg3UkS8qx7+qUZn1c1nOpYgW7AE1cxuBzSM3O/4pyaSnnMGgeUcz/utv+F272rn
/rdDaC1nvH09OKIJOqBxOQ7m7izTBu70P1zhuWmGDAzmvy1sNCUpv325iFBc7B78
fRvINps878aSqheJqIx2jpeykW+nBjbVpsh++0ZUNjoWQTbZM7WaxNJxD4KjdInW
zvK24qX34aMrY4pS0BjpQ46RTkEIDFnzSYTUAN+33LQ9rQ+1DaUF0UJAlO10XBQ+
6J1ZDXnSmqOsXu2pnRyXWKrsliz6+j3LOzkJoc2gQFwiDzex20ZJtO3Jd2dVMJ5a
F/jN5SY800LhvCbPFPL4k03xK98n7fLs432jsJOMYtRvY9N62oEbufBj0dCS0S15
A7Vj537ziRZuGt4xz3vdE48GEBdxm+frPNadS8IurW1gDN4Rr0d5VLfKFwMsiSXr
baVMWTjn6kcfpomYDhl5451lDAyhZ20qFxx9M1lRNj7ploz4khmdv1e1zqENocQd
t4eQrptk4YUgxEIZ0R56b2qf
=h/Vp
-----END PGP SIGNATURE-----
```