



Remote code execution via malicious DHCP options

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-42511
State	PUBLISHED
Assigner	freebsd
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 07:16:37 UTC
Updated	2026-04-30 07:16:37 UTC
Description	The BOOTP file field is written to the lease file without escaping embedded double-quotes, allowing injection of arbitrary dh

Risk And Classification

Problem Types: CWE-149 | CWE-149 CWE-149: Improper Neutralization of Quoting Syntax

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FreeBSD	FreeBSD	affected 15.0-RELEASE p7 release	Not specified
CNA	FreeBSD	FreeBSD	affected 14.4-RELEASE p3 release	Not specified
CNA	FreeBSD	FreeBSD	affected 14.3-RELEASE p12 release	Not specified
CNA	FreeBSD	FreeBSD	affected 13.5-RELEASE p13 release	Not specified

References

Reference	Source	Link	Tags
security.freebsd.org/advisories/FreeBSD-SA-26:12.dhclient.asc	secteam@freebsd.org	security.freebsd.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Joshua Rogers of AISLE Research Team (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)