INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-03 06:18 UTC

CVE-2026-42511: The BOOTP file field is written to the lease file without escaping embedded double-quotes, allowing ...

CVE VULNERABILITY | HIGH | CVSS 8.1

SCC Item ID	SCC-CVE-2026-0113
Type	CVE Vulnerability
CVE ID	CVE-2026-42511
Severity	HIGH
CVSS Base Score	8.1
EPSS Score	0.0004 (14th percentile)
Affected Products	FreeBSD (dhclient), specific versions not enumerated in source data
Published	2026-04-30T07:16:37.290
Discovery Source	Nvd

Executive Summary

CVE-2026-42511 is a high-severity code injection vulnerability in the FreeBSD dhclient DHCP client. A rogue DHCP server can inject arbitrary directives into a system's lease file, which are then executed as root when the system restarts or renews its lease. Any FreeBSD system that obtains network configuration via DHCP is potentially exposed, with the highest risk in untrusted or shared network environments.

Technical Analysis

CVE-2026-42511 (CWE-149: Improper Neutralization of Quoting Syntax) affects FreeBSD's dhclient implementation. The BOOTP 'file' field received from a DHCP server is written to the lease file (/var/db/dhclient.leases) without sanitizing embedded double-quote characters. On subsequent lease file re-parsing, triggered by system restart or lease renewal, dhclient passes the unsanitized field value to dhclient-script(8), which evaluates it as shell input. This permits a rogue DHCP server to inject arbitrary dhclient.conf directives and achieve root-level code execution on the client. Attack path maps to MITRE ATT&CK T1557 (Adversary-in-the-Middle, for DHCP spoofing/rogue server positioning), T1203 (Exploitation for Client Execution), and T1059 (Command and Scripting Interpreter). CVSS base score: 8.1. EPSS score: 0.00045 (13.6th percentile), low observed exploitation activity at time of publication. Specific affected FreeBSD versions are not enumerated in available source data; check FreeBSD Security Advisories for confirmed version scope. CISA KEV: not listed.

Action Checklist

1. Containment: Identify all FreeBSD systems in your environment running dhclient. Prioritize systems on untrusted, shared, or externally accessible network segments (guest Wi-Fi, co-location, cloud VPC shared subnets). Where operationally feasible, temporarily configure static IP addressing on high-value systems to bypass DHCP until a patch is applied.
2. Detection: Query asset inventory for FreeBSD hosts using dhclient. Review /var/db/dhclient.leases on affected hosts for unexpected or malformed 'file' field values containing quote characters, shell metacharacters, or unusual directive syntax. Correlate DHCP server logs for unexpected OFFER or ACK packets from unauthorized DHCP server MAC/IP addresses. Alert on dhclient-script(8) process execution spawning unexpected child processes.
3. Eradication: Apply the FreeBSD security patch addressing CVE-2026-42511 as published in the FreeBSD Security Advisory (check https://security.freebsd.org/advisories/ for the relevant SA). If no patch is yet available for your version, restrict DHCP to trusted network segments via firewall ACLs and enable DHCP snooping on managed switches where supported. Rotate any credentials or secrets accessible to root on affected hosts that may have been exposed.
4. Recovery: After patching, verify the corrected dhclient binary version matches the advisory's patched version. Re-examine /var/db/dhclient.leases for residual malicious directives and purge the file before renewing leases. Monitor dhclient-script(8) execution and root-level process spawning for 72 hours post-remediation to confirm no persistence mechanisms were installed.
5. Post-Incident: This vulnerability exposes a gap in DHCP trust controls. Evaluate deployment of 802.1X port authentication or DHCP snooping to prevent rogue DHCP server positioning. Review network segmentation to ensure FreeBSD hosts do not reside on segments where untrusted devices can respond to DHCP broadcasts. Document FreeBSD systems in your CMDB with OS and DHCP client details to accelerate future triage.

Detection Guidance

Primary indicators: (1) Inspect /var/db/dhclient.leases on FreeBSD hosts for 'file' field values containing double-quote characters ("), semicolons, or shell metacharacters - these are not expected in normal BOOTP file field values. (2) Use packet capture or DHCP server logs to identify DHCP OFFER or ACK packets sourced from MAC/IP addresses not matching your authorized DHCP infrastructure; rogue server activity on the segment is a prerequisite for exploitation. (3) Monitor process execution logs (e.g., auditd or DTrace on FreeBSD) for dhclient-script(8) spawning unexpected child processes, particularly shells (/bin/sh, /bin/csh) with unusual arguments. (4) Alert on new cron jobs, rc.d scripts, or suid binaries created around the time of a lease renewal or system restart, potential indicators of post-exploitation persistence. MITRE ATT&CK T1557 (DHCP spoofing) detection requires network-layer visibility; endpoint-only monitoring will not catch the initial rogue server activity.

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution

- **T1557** — Adversary-in-the-Middle
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1557	Adversary-in-the-Middle	Credential-Access
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-42511	T1
CVE-2026-42511 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-42511	T3
CVE-2026-42511 - Security Bug Tracker - Debian	https://security-tracker.debian.org/tracker/CVE-2026-42511	T3
CVE-2026-42511 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-42511	T3
CVE-2026-42511 CPEs | Tenable®	https://www.tenable.com/cve/CVE-2026-42511/cpes	T3

Generated 2026-05-03 06:18 UTC by TJS Security Command Center