



CVE-2018-16227

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-16227
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-03 16:15:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	The IEEE 802.11 parser in tcpdump before 4.9.3 has a buffer over-read in print-802_11.c for the Mesh Flags subfield.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Tcpdump	Tcpdump	All	All	All	All
Application	Tcpdump	Tcpdump	All	All	All	All

References

Reference

[security-announce] openSUSE-SU-2019:2344-1: important: Security update

Debian -- Security Information -- DSA-4547-1 tcpdump

[SECURITY] Fedora 29 Update: tcpdump-4.9.3-1.fc29 - package-announce - Fedora Mailing-Lists

Full Disclosure: APPLE-SA-2019-12-10-3 macOS Catalina 10.15.2, Security Update 2019-002 Mojave, Security Update 2019-007 High Sierra

[SECURITY] Fedora 29 Update: tcpdump-4.9.3-1.fc29 - package-announce - Fedora Mailing-Lists

USN-4252-1: tcpdump vulnerabilities | Ubuntu security notices

October 2019 Tcpdump Vulnerabilities in NetApp Products | NetApp Product Security

[SECURITY] Fedora 31 Update: tcpdump-4.9.3-1.fc31 - package-announce - Fedora Mailing-Lists

tcpdump/CHANGES at tcpdump-4.9 · the-tcpdump-group/tcpdump · GitHub

USN-4252-2: tcpdump vulnerabilities | Ubuntu security notices

About the security content of macOS Catalina 10.15.2, Security Update 2019-002 Mojave, Security Update 2019-007 High Sierra - Apple Support

[SECURITY] [DLA 1955-1] tcpdump security update

(for 4.9.3) CVE-2018-16227/IEEE 802.11: add a missing bounds check · the-tcpdump-group/tcpdump@4846b3c · GitHub

[SECURITY] Fedora 30 Update: tcpdump-4.9.3-1.fc30 - package-announce - Fedora Mailing-Lists

[security-announce] openSUSE-SU-2019:2348-1: important: Security update

[SECURITY] Fedora 30 Update: tcpdump-4.9.3-1.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 31 Update: tcpdump-4.9.3-1.fc31 - package-announce - Fedora Mailing-Lists

Bugtraq: [SECURITY] [DSA 4547-1] tcpdump security update

Bugtraq: APPLE-SA-2019-12-10-3 macOS Catalina 10.15.2, Security Update 2019-002 Mojave, Security Update 2019-007 High Sierra

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

376142 F5 BIG-IP Local Traffic Manager (LTM), Application Security Manager (ASM), Access Policy Manager (APM) Multiple

Vulnerabilities (K44551633)

[500686](#) Alpine Linux Security Update for tcpdump

[504455](#) Alpine Linux Security Update for tcpdump

[940081](#) AlmaLinux Security Update for tcpdump (ALSA-2020:4760)

[960865](#) Rocky Linux Security Update for tcpdump (RLSA-2020:4760)

© [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](#).

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