CVE-2017-11108

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-11108
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-08 17:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	tcpdump 4.9.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tcpdump	Tcpdump	4.9.0	All	All	All
Application	Tcpdump	Tcpdump	4.9.0	All	All	All

References

Reference
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
Tcpdump: Multiple vulnerabilities (GLSA 201709-23) — Gentoo security
Debian -- Security Information -- DSA-3971-1 tcpdump
Red Hat Customer Portal
Bug 1468504 – There is a heap buffer overflow tcpdump. A crafted input will lead to remote denial of service attack.
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500685 Alpine Linux Security Update for tcpdump

504454 Alpine Linux Security Update for tcpdump

671059 EulerOS Security Update for tcpdump (EulerOS-SA-2019-2435)

710483 Gentoo Linux Tcpdump Multiple Vulnerabilities (GLSA 201709-23)