CVE-2017-13028

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

Summary

CVE	CVE-2017-13028
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-14 06:29:00 UTC
Updated	2020-10-28 19:23:00 UTC
Description	The BOOTP parser in tcpdump before 4.9.2 has a buffer over-read in print-bootp.c:bootp_print().

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
www.tcpdump.org/tcpdump-changes.txt
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
CVE-2017-13028/BOOTP: Add another test. · the-tcpdump-group/tcpdump@66e2296 · GitHub
Tcpdump: Multiple vulnerabilities (GLSA 201709-23) — Gentoo security
Debian -- Security Information -- DSA-3971-1 tcpdump
Tcpdump Multiple Flaws Let Remote Users View Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracke
Red Hat Customer Portal
CVE-2017-13028/BOOTP: Add a bounds check before fetching data · the-tcpdump-group/tcpdump@29e5470 · GitHub

CVE-2017-13028/BOOTP: Add a bounds check before fetching data · the-tcpdump-group/tcpdump@29e5470 · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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