



CVE-2017-12896

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

Summary

CVE	CVE-2017-12896
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-14 06:29:00 UTC
Updated	2020-10-23 18:17:00 UTC
Description	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:isakmp_rfc3948_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	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	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

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

Tcpdump Multiple Flaws Let Remote Users View Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracke

Red Hat Customer Portal

CVE-2017-12896/ISAKMP: Add another test. · the-tcpdump-group/tcpdump@4e430c6 · GitHub

CVE-2017-12896/ISAKMP: Do bounds checks in isakmp_rfc3948_print(). · the-tcpdump-group/tcpdump@f76e7fe · 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)

© [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](#)