



CVE-2003-0989

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

Summary

CVE	CVE-2003-0989
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-02-17 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	tcpdump before 3.8.1 allows remote attackers to cause a denial of service (infinite loop) via certain ISAKMP packets, a difference between the implementation and the specification.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

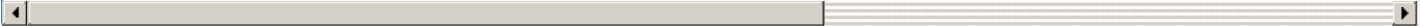
AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Linux	9.0	All	i386	All

Application	Redhat	Tcpdump	All	All	All
Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	
References					
Reference				Source	
Repository / Oval Repository				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - Trustix update for tcpdump				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - OpenLinux update for tcpdump				af854a3a-2127-422b-91ae-364da	
CERT/CC Vulnerability Note VU#738518				af854a3a-2127-422b-91ae-364da	
'[FLSA-2004:1222] Updated tcpdump resolves security vulnerabilites (resend with correct paths)' - MARC				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - Fedora update for tcpdump				af854a3a-2127-422b-91ae-364da	
SecurityFocus				af854a3a-2127-422b-91ae-364da	
redhat.com Red Hat, Inc.				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - tcpdump ISAKMP and RADIUS Packet Handling Vulnerabilities				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - Red Hat update for tcpdump				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - Debian update for tcpdump				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - Mandrake update for tcpdump				af854a3a-2127-422b-91ae-364da	
Debian -- Security Information -- DSA-425-1 tcpdump				af854a3a-2127-422b-91ae-364da	
redhat.com Red Hat Support				af854a3a-2127-422b-91ae-364da	
LWN: EnGarde alert ESA-20040119-002 (tcpdump)				af854a3a-2127-422b-91ae-364da	
APPLE-SA-2004-02-23 Security Update 2004-02-23				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - EnGarde update for tcpdump				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - UnixWare update for tcpdump				af854a3a-2127-422b-91ae-364da	
Mandriva Security Advisories				af854a3a-2127-422b-91ae-364da	
patches.sgi.com/support/free/security/advisories/20040202-01-U.asc				af854a3a-2127-422b-91ae-364da	
Tcpdump Can Be Crashed By a Remote User Sending a Malicious ISAKMP Packet - SecurityTracker				af854a3a-2127-422b-91ae-364da	
Repository / Oval Repository				af854a3a-2127-422b-91ae-364da	
redhat.com Red Hat, Inc.				af854a3a-2127-422b-91ae-364da	
TCPDump ISAKMP Decoding Routines Denial Of Service Vulnerability				af854a3a-2127-422b-91ae-364da	
Secunia - Advisories - SuSE update for tcpdump				af854a3a-2127-422b-91ae-364da	
redhat.com Red Hat, Inc.				af854a3a-2127-422b-91ae-364da	
redhat.com Red Hat Support				af854a3a-2127-422b-91ae-364da	
Repository / Oval Repository				af854a3a-2127-422b-91ae-364da	
LWN: Trustix alert 2004-0004 (tcpdump)				af854a3a-2127-422b-91ae-364da	

LWN: Trusux alert 2004-0004 (lcpdump)	af854a3a-2127-422b-91ae-364da
ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.9/SCOSA-2004.9.txt	af854a3a-2127-422b-91ae-364da
patches.sgi.com/support/free/security/advisories/20040103-01-U.asc	af854a3a-2127-422b-91ae-364da
ftp.sco.com/pub/security/OpenLinux/CSSA-2004-008.0.txt	af854a3a-2127-422b-91ae-364da
redhat.com Red Hat, Inc.	af854a3a-2127-422b-91ae-364da
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.