



CVE-2001-1279

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2001-1279
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-07-17 04:00:00 UTC
Updated	2008-09-10 19:10:00 UTC
Description	Buffer overflow in print-rx.c of tcpdump 3.x (probably 3.6x) allows remote attackers to cause a denial of service and possibly

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lbl	Tcpdump	3.6.2	All	All	All
Application	Lbl	Tcpdump	3.6.2	All	All	All

References

Reference	Source
CERT/CC Vulnerability Note VU#797201	CERT-VN
ISS X-Force Database: tcpdump-afs-rcp-bo (7006): tcpdump AFS RCP packet buffer overflow could allow root level access	XF
FreeBSD-SA-01:48	FREEBSD
CSSA-2002-025.0	CALDERA
redhat.com Red Hat Support	REDHAT
MandrakeSoft Security Advisory MDKSA-2002:032 : tcpdump	MANDRAKE
TCPDump AFS Signed Integer Buffer Overflow Vulnerability	BID
Home - Conectiva	CONNECTIVA
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.

© [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](#)