CVE-2007-1218

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

Summary

CVE	CVE-2007-1218
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-02 21:18:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Off-by-one buffer overflow in the parse_elements function in the 802.11 printer code (print-802_11.c) for tcpdump 3.9.5 and

Risk And Classification

Problem Types: CWE-119 | CWE-189

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
SecurityTracker.com Archives - Tcpdump Off-by-One Heap Overflow Lets Remote Users Deny Service	SECTRACK	www.securitytracker.c
tcpdump IEEE802.11 Printer Remote Buffer Overflow Vulnerability	BID	www.securityfocus.co
Webmail - OVH	VUPEN	www.vupen.com
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com
168916 – net-analyzer/tcpdump off-by-one heap overflow in 802.11 printer (CVE-2007-1218)	MISC	bugs.gentoo.org
CVS log for tcpdump/print-802_11.c	CONFIRM	cvs.tcpdump.org
US-CERT Technical Cyber Security Alert TA07-352A -- Apple Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov
About Security Update 2007-009	CONFIRM	docs.info.apple.com
32427	OSVDB	www.osvdb.org
APPLE-SA-2007-12-17 Security Update 2007-009	APPLE	lists.apple.com
Debian update for tcpdump - Advisories - Secunia	SECUNIA	secunia.com
404 Not Found	TURBO	www.turbolinux.com
Advisories | Mandriva	MANDRIVA	www.mandriva.com

Ubuntu update for tcpdump - Advisories - Secunia	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
[SECURITY] Fedora Core 6 Update: tcpdump-3.9.4-10.fc6 | FedoraNEWS.ORG	FEDORA	fedoranews.org
IBM X-Force Exchange	XF	exchange.xforce.ibm
cvs.tcpdump.org/cgi-bin/cvsweb/tcpdump/print-802_11.c	MISC	cvs.tcpdump.org
Advisories | Mandriva	MANDRIVA	www.mandriva.com
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
[SECURITY] Fedora Core 5 Update: tcpdump-3.9.4-4.fc5 | FedoraNEWS.ORG	FEDORA	fedoranews.org
Mandriva update for tcpdump - Advisories - Secunia	SECUNIA	secunia.com
Full Disclosure: tcpdump: off-by-one heap overflow in 802.11 printer	FULLDISC	seclists.org
issues.rpath.com/browse/RPL-1100	CONFIRM	issues.rpath.com
Debian -- Security Information -- DSA-1272-1 tcpdump	DEBIAN	www.debian.org
USN-429-1: tcpdump vulnerability | Ubuntu	UBUNTU	www.ubuntu.com
Fedora update for tcpdump - Advisories - Secunia	SECUNIA	secunia.com
tcpdump 802.11 "parse_elements()" Off-By-One Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Red Hat update for tcpdump - Advisories - Secunia	SECUNIA	secunia.com
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
rpath update for tcpdump - Advisories - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-05-11	Mark J Cox	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/

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