CVE-2007-3798

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-3798
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-16 22:30:00 UTC
Updated	2024-01-12 22:06:00 UTC
Description	Integer overflow in print-bgp.c in the BGP dissector in tcpdump 3.9.6 and earlier allows remote attackers to execute arbitrar

Risk And Classification

Problem Types: CWE-252

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	5.5	-	All	All
Operating System	Freebsd	Freebsd	5.5	p1	All	All
Operating System	Freebsd	Freebsd	5.5	p11	All	All
Operating System	Freebsd	Freebsd	5.5	p12	All	All
Operating System	Freebsd	Freebsd	5.5	p13	All	All
Operating System	Freebsd	Freebsd	5.5	p14	All	All
Operating System	Freebsd	Freebsd	5.5	p2	All	All
Operating System	Freebsd	Freebsd	5.5	p3	All	All
Operating System	Freebsd	Freebsd	5.5	p4	All	All

Operating System	Freebsd	Freebsd	5.5	p5	All	All
Operating System	Freebsd	Freebsd	5.5	p7	All	All
Operating System	Freebsd	Freebsd	5.5	p8	All	All
Operating System	Freebsd	Freebsd	5.5	p9	All	All
Operating System	Freebsd	Freebsd	6.1	-	All	All
Operating System	Freebsd	Freebsd	6.1	p1	All	All
Operating System	Freebsd	Freebsd	6.1	p10	All	All
Operating System	Freebsd	Freebsd	6.1	p11	All	All
Operating System	Freebsd	Freebsd	6.1	p12	All	All
Operating System	Freebsd	Freebsd	6.1	p13	All	All
Operating System	Freebsd	Freebsd	6.1	p16	All	All
Operating System	Freebsd	Freebsd	6.1	p17	All	All
Operating System	Freebsd	Freebsd	6.1	p18	All	All
Operating System	Freebsd	Freebsd	6.1	p2	All	All
Operating System	Freebsd	Freebsd	6.1	p4	All	All
Operating System	Freebsd	Freebsd	6.1	p6	All	All
Operating System	Freebsd	Freebsd	6.1	p7	All	All
Operating System	Freebsd	Freebsd	6.1	p9	All	All
Operating System	Freebsd	Freebsd	6.2	-	All	All
Operating System	Freebsd	Freebsd	6.2	p1	All	All
Operating System	Freebsd	Freebsd	6.2	p4	All	All
Operating System	Freebsd	Freebsd	6.2	p5	All	All
Operating System	Freebsd	Freebsd	6.2	p6	All	All
Application	Slackware	Slackware	10.0	All	All	All
Application	Slackware	Slackware	10.1	All	All	All
Application	Slackware	Slackware	10.2	All	All	All
Application	Slackware	Slackware	11.0	All	All	All
Application	Slackware	Slackware	12.0	All	All	All
Application	Slackware	Slackware	9.0	All	All	All
Application	Slackware	Slackware	9.1	All	All	All
Application	Tcpdump	Tcpdump	All	All	All	All

References

Reference	Source	Link
FreeBSD-SA-07:06	FREEBSD	secur

Debian -- Security Information -- DSA-1353-1 tcpdump	DEBIAN	www.d
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secun
FreeBSD update for tcpdump - Advisories - Secunia	SECUNIA	secun
Repository / Oval Repository	OVAL	oval.c
US-CERT Technical Cyber Security Alert TA07-352A -- Apple Updates for Multiple Vulnerabilities	CERT	www.u
Gentoo Bug 184815 - net-analyzer/tcpdump <= 3.9.6 BGP dissector integer overflow (CVE-2007-3798)	CONFIRM	bugs.g
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	secun
Gentoo update for tcpdump - Advisories - Secunia	SECUNIA	secun
About Security Update 2007-009	CONFIRM	docs.i
Slackware update for tcpdump - Advisories - Secunia	SECUNIA	secun
SecurityTracker.com Archives - Tcpdump Buffer Overflow in 'print-bgp.c' Lets Remote Users Execute Arbitrary Code	SECTRACK	www.s
APPLE-SA-2007-12-17 Security Update 2007-009	APPLE	lists.a
cvs.tcpdump.org/cgi-bin/cvsweb/tcpdump/print-bgp.c	MISC	cvs.tc
USN-492-1: tcpdump vulnerability | Ubuntu	UBUNTU	www.u
tcpdump Print-bgp.C Remote Integer Underflow Vulnerability	BID	www.s
tcpdump print-bgp.c Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secun
404 Not Found	TURBO	www.t
2007-0023	TRUSTIX	www.t
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.v
Mandriva update for tcpdump - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
rPath update for tcpdump - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
Ubuntu update for tcpdump - Advisories - Secunia	SECUNIA	secun
Debian update for tcpdump - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
rhn.redhat.com | Red Hat Support	REDHAT	www.r
Webmail - OVH	VUPEN	www.v
Trustix Update for Multiple Packages - Advisories - Secunia	SECUNIA	secun
Gentoo Linux Documentation -- tcpdump: Integer overflow	GENTOO	secur
SecurityFocus	BUGTRAQ	www.s
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	slackv
Security Announcement	SUSE	www.n
www.digit-labs.org/files/exploits/private/tcpdump-bgp.c	MISC	www.d
Red Hat update for tcpdump - Advisories - Secunia	SECUNIA	secun
rhn.redhat.com | Red Hat Support	REDHAT	www.r
Advisories | Mandriva	MANDRIVA	www.m
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-07-31	Joshua Bressers	This issue does not affect the version of tcpdump shipped in Red Hat Enterprise Linux 2.1 o

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