



# CVE-2007-3798

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-3798
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-07-16 22:30:00 UTC
<b>Updated</b>	2024-01-12 22:06:00 UTC
<b>Description</b>	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	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X Server</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	7.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	All	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	-	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p1	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p11	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p12	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p13	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p14	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p2	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p3	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p4	All	All

Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p5	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p7	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p8	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	5.5	p9	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	-	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p1	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p10	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p11	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p12	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p13	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p16	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p17	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p18	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p2	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p4	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p6	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p7	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.1	p9	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.2	-	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.2	p1	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.2	p4	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.2	p5	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	6.2	p6	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	10.0	All	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	10.1	All	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	10.2	All	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	11.0	All	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	12.0	All	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	9.0	All	All	All
Application	<a href="#">Slackware</a>	<a href="#">Slackware</a>	9.1	All	All	All
Application	<a href="#">Tcpcdump</a>	<a href="#">Tcpcdump</a>	All	All	All	All

## References

Reference	Source	Link
FreeBSD-SA-07:06	FREEBSD	<a href="#">secu</a>
...	...	...

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

## 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.

© [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](#)