



CVE-2012-1596

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-1596
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-11 10:39:00 UTC
Updated	2017-12-29 02:29:00 UTC
Description	The mp2t_process_fragmented_payload function in epan/dissectors/packet-mp2t.c in the MP2T dissector in Wireshark 1.4.

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.11	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All

Application	Wireshark	Wireshark	1.6.5	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.11	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.6.5	All	All	All

References						
Reference			Source		Link	
Wireshark ANSI A/IEEE 802.11/PCAP/MP2T Bugs Let Remote Users Deny Service - SecurityTracker			SECTrack		www.securitytracker.com	
Wireshark MP2T Dissector Denial of Service Vulnerability			BID		www.securityfocus.com	
[Wireshark] Revision 41001			CONFIRM		anonsvn.wireshark.org	
[SECURITY] Fedora 15 Update: wireshark-1.4.12-1.fc15			FEDORA		lists.fedoraproject.org	
Repository / Oval Repository			OVAL		oval.cisecurity.org	
Security Alerts - Secunia			SECUNIA		secunia.com	
6833 – Buildbot crash output: fuzz-2012-02-10-14752.pcap			CONFIRM		bugs.wireshark.org	
Security Alerts - Secunia			SECUNIA		secunia.com	
openSUSE-SU-2012:0558-1: moderate: update for wireshark			SUSE		lists.opensuse.org	
[SECURITY] Fedora 16 Update: wireshark-1.6.6-1.fc16			FEDORA		lists.fedoraproject.org	
Wireshark · wnpa-sec-2012-07			CONFIRM		www.wireshark.org	
IBM X-Force Exchange			XF		exchange.xforce.ibmcloud.com	
oss-security - Re: CVE Request: Multiple wireshark security flaws resolved in 1.4.12 and 1.6.6			MLIST		www.openwall.com	
CVE-2012-0702			CVE-2012-0702			

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report