



CVE-2017-15189

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

Summary

CVE	CVE-2017-15189
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-10 21:29:00 UTC
Updated	2023-11-07 02:39:00 UTC
Description	In Wireshark 2.4.0 to 2.4.1, the DOCSIS dissector could go into an infinite loop. This was addressed in plugins/docsis/pack

Risk And Classification

Problem Types: CWE-772

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	2.4.0	All	All	All
Application	Wireshark	Wireshark	2.4.1	All	All	All
Application	Wireshark	Wireshark	2.4.0	All	All	All
Application	Wireshark	Wireshark	2.4.1	All	All	All

References

Reference	Source	Link	Tags
Gerrit Code Review	CONFIRM	code.wireshark.org	Patch, Vendor
code.wireshark Code Review - wireshark.git/commit	CONFIRM	code.wireshark.org	Patch, Vendor
14080 – Buildbot crash output: fuzz-2017-09-22-1295.pcap	CONFIRM	bugs.wireshark.org	Issue Tracking
Wireshark DOCSIS Dissector '/docsis/packet-docsis.c' Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Ad
Wireshark · wnpa-sec-2017-46 · DOCSIS infinite loop	CONFIRM	www.wireshark.org	Vendor Adviso
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)