



# CVE-2018-18227

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

## Summary

<b>CVE</b>	CVE-2018-18227
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-10-12 06:29:00 UTC
<b>Updated</b>	2023-11-07 02:55:00 UTC
<b>Description</b>	In Wireshark 2.6.0 to 2.6.3 and 2.4.0 to 2.4.9, the MS-WSP protocol dissector could crash. This was addressed in epan/dis

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

### Reference

<a href="#">code.wireshark Code Review - wireshark.git/commit</a>
<a href="#">Debian -- Security Information -- DSA-4359-1 wireshark</a>
<a href="#">code.wireshark Code Review - wireshark.git/commit</a>
<a href="#">Wireshark MS-WSP/Steam IHS Discovery/CoAP/OpcUa Processing Bugs Lets Remote Users Cause the Target Service to Crash - SecurityTr</a>
<a href="#">[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f</a>
<a href="#">15119 – Buildbot crash output: fuzz-2018-09-07-29306.pcap</a>
<a href="#">Oracle Critical Patch Update Advisory - April 2020</a>
<a href="#">Wireshark Multiple Denial of Service Vulnerabilities</a>
<a href="#">Wireshark · wnpa-sec-2018-47 · MS-WSP dissector crash</a>
<a href="#">CVE Program record</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

501312 Alpine Linux Security Update for wireshark

© [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](#)**