CVE-2018-18227

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-18227
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-12 06:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	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	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

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

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501312 Alpine Linux Security Update for wireshark