CVE-2016-4077

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-4077
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-25 10:59:00 UTC
Updated	2023-11-07 02:32:00 UTC
Description	epan/reassemble.c in TShark in Wireshark 2.0.x before 2.0.3 relies on incorrect special-case handling of truncated Tvb data

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All

References

Reference	Source	Link	Tags
651 - project-zero - Project Zero - Monorail	MISC	code.google.com	Exploit
code.wireshark Code Review - wireshark.git/commit	CONFIRM	code.wireshark.org	
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
Wireshark Multiple Dissector Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com	
Wireshark · wnpa-sec-2016-20 · TShark reassembly crash	CONFIRM	www.wireshark.org	Vendor Ad
Bug 11799 – Wireshark use-after-free in print_hex_data_buffer / print_packet	CONFIRM	bugs.wireshark.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

671108 EulerOS Security Update for wireshark (EulerOS-SA-2019-2425)