CVE-2017-9345

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-9345
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-02 05:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DNS dissector could go into an infinite loop. This was addressed in epar

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Wireshark 'epan/dissectors/packet-dns.c' Denial of Service Vulnerability	BID	www.securityfocus.com	Third Pa
13633 – [oss-fuzz] timeout: expand_dns_name epan/dissectors/packet-dns.c:1158:21	MISC	bugs.wireshark.org	Issue Tra
code.wireshark Code Review - wireshark.git/commit	MISC	code.wireshark.org	Issue Tra
Wireshark · wnpa-sec-2017-26 · DNS dissector infinite loop	MISC	www.wireshark.org	Vendor A
Wireshark Multiple Dissector Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com	Third Pa
1206 - wireshark: Timeout in wireshark_fuzzshark_udp_port-bootp - oss-fuzz - Monorail	MISC	bugs.chromium.org	Issue Tra
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501301 Alpine Linux Security Update for wireshark

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