CVE-2015-3810

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-3810
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-26 15:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	epan/dissectors/packet-websocket.c in the WebSocket dissector in Wireshark 1.12.x before 1.12.5 uses a recursive algorith

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.12.2	All	All	All
Application	Wireshark	Wireshark	1.12.3	All	All	All
Application	Wireshark	Wireshark	1.12.4	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.12.2	All	All	All
Application	Wireshark	Wireshark	1.12.3	All	All	All
Application	Wireshark	Wireshark	1.12.4	All	All	All

References

Reference	Source	Link	Tags
Wireshark Websocket Dissector CVE-2015-3810 Denial of Service Vulnerability	BID	www.securityfocus.com	
Wireshark · wnpa-sec-2015-13 · WebSocket DoS	CONFIRM	www.wireshark.org	Vendor Advisory
Debian -- Security Information -- DSA-3277-1 wireshark	DEBIAN	www.debian.org	
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle.com	

Bug 10989 – Websocket: deep recursion (DoS?)	CONFIRM	bugs.wireshark.org	
Wireshark: Multiple vulnerabilities (GLSA 201510-03) — Gentoo Security	GENTOO	security.gentoo.org	
code.wireshark Code Review - wireshark.git/commit	CONFIRM	code.wireshark.org	
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, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.