



CVE-2017-11408

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

Summary

CVE	CVE-2017-11408
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-18 21:29:00 UTC
Updated	2023-11-07 02:38:00 UTC
Description	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the AMQP dissector could crash. This was addressed in epan/dissectors/pa

Risk And Classification

Problem Types: CWE-20

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	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.12	All	All	All
Application	Wireshark	Wireshark	2.0.13	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	2.0.4	All	All	All
Application	Wireshark	Wireshark	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All

Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All
Application	Wireshark	Wireshark	2.2.5	All	All	All
Application	Wireshark	Wireshark	2.2.6	All	All	All
Application	Wireshark	Wireshark	2.2.7	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.12	All	All	All
Application	Wireshark	Wireshark	2.0.13	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	2.0.4	All	All	All
Application	Wireshark	Wireshark	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All
Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All
Application	Wireshark	Wireshark	2.2.5	All	All	All
Application	Wireshark	Wireshark	2.2.6	All	All	All
Application	Wireshark	Wireshark	2.2.7	All	All	All

References						
Reference						Source
Wireshark AMQP/MQ/DOCSIS/GPRS LLC Dissector Bugs Let Remote Users Cause the Target Service to Crash - SecurityTracker						SECTR
code.wireshark Code Review - wireshark.git/commit						
[SECURITY] [DLA 1226-1] wireshark security update						MLIST
Wireshark AMQP Dissector CVE-2017-11408 Denial of Service Vulnerability						BID
Debian -- Security Information -- DSA-4060-1 wireshark						DEBIAN

code.wireshark Code Review - wireshark.git/commit	
Wireshark · wnpa-sec-2017-34 · AMQP dissector crash	CONFIF
13780 – [oss-fuzz] ASAN: stack-overflow (/usr/lib/libc.so.6+0x48a85) in _IO_vfprintf_internal	CONFIF
code.wireshark Code Review - wireshark.git/commit	CONFIF
code.wireshark Code Review - wireshark.git/commit	CONFIF
CVE Program record	CVE.OF
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings	
501302 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)