



CVE-2017-7746

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

Summary

CVE	CVE-2017-7746
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-12 23:59:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the SLSK dissector could go into an infinite loop, triggered by packet injectio

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	2.0.2	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	2.0.0	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	2.0.2	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

References				
Reference	Source	Link	Tag	
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org		
code.wireshark Code Review - wireshark.git/commit	CONFIRM	code.wireshark.org	Issu	
Wireshark SLSK Dissector 'dissectors/packet-slsk.c' Infinite Loop Denial of Service Vulnerability	BID	www.securityfocus.com	Thir	
Wireshark · wnpa-sec-2017-19 · SLSK dissector long loop	CONFIRM	www.wireshark.org	Ven	
[SECURITY] [DLA 1634-1] wireshark security update	MLIST	lists.debian.org	Mail	
13576 – libfuzzer: SLSK long dissector loop	CONFIRM	bugs.wireshark.org	Issu	
CVE Program record	CVE.ORG	www.cve.org	can	
NVD vulnerability detail	NVD	nvd.nist.gov	can	

No vendor comments have been submitted for this CVE.

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

© [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](#)