



CVE-2019-10898

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

Summary

CVE	CVE-2019-10898
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-09 04:29:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	In Wireshark 3.0.0, the GSUP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-gsm_g

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Wireshark	Wireshark	3.0.0	All	All	All
Application	Wireshark	Wireshark	3.0.0	All	All	All

References

Reference	Source	Link	
15585 – [oss-fuzz] #13232: Timeout in wireshark_fuzzshark_ip	MISC	bugs.wireshark.org	E
[SECURITY] Fedora 29 Update: wireshark-3.0.1-1.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 30 Update: wireshark-3.0.1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M
Wireshark · wnpa-sec-2019-12 · GSUP dissector infinite loop	MISC	www.wireshark.org	\
[SECURITY] Fedora 29 Update: wireshark-3.0.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M
code.wireshark Code Review - wireshark.git/commit	MISC	code.wireshark.org	F
Wireshark Multiple Denial of Service Vulnerabilities	BID	www.securityfocus.com	1
[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f	SUSE	lists.opensuse.org	

[SECURITY] Fedora 30 Update: wireshark-3.0.1-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c
No vendor comments have been submitted for this CVE.			
Legacy QID Mappings			
501317 Alpine Linux Security Update for wireshark			

© [CVE.report](https://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