



# CVE-2019-10894

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

## Summary

<b>CVE</b>	CVE-2019-10894
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-09 04:29:00 UTC
<b>Updated</b>	2023-11-07 03:02:00 UTC
<b>Description</b>	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the GSS-API dissector could crash. This was addressed in epan/diss

## Risk And Classification

**Problem Types:** CWE-617

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	3.0.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	3.0.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

Reference	Source	Link	T
code.wireshark Code Review - wireshark.git/commit		<a href="https://code.wireshark.org">code.wireshark.org</a>	
[SECURITY] Fedora 29 Update: wireshark-3.0.1-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Wireshark · wnpa-sec-2019-14 · GSS-API dissector crash	MISC	<a href="https://www.wireshark.org">www.wireshark.org</a>	F
[SECURITY] Fedora 30 Update: wireshark-3.0.1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	M
[SECURITY] [DLA 2423-1] wireshark security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
code.wireshark Code Review - wireshark.git/commit	MISC	<a href="https://code.wireshark.org">code.wireshark.org</a>	F
[SECURITY] Fedora 29 Update: wireshark-3.0.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	M
[SECURITY] [DLA 1802-1] wireshark security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[security-announce] openSUSE-SU-2019:1356-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Wireshark Multiple Denial of Service Vulnerabilities	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	T
[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
USN-3986-1: Wireshark vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
[security-announce] openSUSE-SU-2019:1390-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[SECURITY] Fedora 30 Update: wireshark-3.0.1-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
15613 – Wireshark assertion failure ("call_dissector_only: assertion failed: (handle != NULL)")	MISC	<a href="https://bugs.wireshark.org">bugs.wireshark.org</a>	E
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	c
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	c

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 501316 Alpine Linux Security Update for wireshark
- 670216 EulerOS Security Update for wireshark (EulerOS-SA-2021-1859)
- 670680 EulerOS Security Update for wireshark (EulerOS-SA-2021-2438)
- 670911 EulerOS Security Update for wireshark (EulerOS-SA-2021-1859)

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)