



# CVE-2022-3190

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

## Summary

<b>CVE</b>	CVE-2022-3190
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-13 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:50:00 UTC
<b>Description</b>	Infinite loop in the F5 Ethernet Trailer protocol dissector in Wireshark 3.6.0 to 3.6.7 and 3.4.0 to 3.4.15 allows denial of serv

## Risk And Classification

### Problem Types: CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

Reference	Source	Link
f5ethtrailer: Infinite loop in legacy style dissector (#18307) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="#">gitlab.com</a>
[SECURITY] Fedora 37 Update: wireshark-4.0.2-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproje</a>
2022/CVE-2022-3190.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
[SECURITY] Fedora 37 Update: wireshark-4.0.2-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproje</a>
[SECURITY] Fedora 36 Update: wireshark-3.6.10-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproje</a>
Wireshark · wnpa-sec-2022-06 · F5 Ethernet Trailer dissector infinite loop	MISC	<a href="#">www.wireshark.</a>
[SECURITY] Fedora 36 Update: wireshark-3.6.10-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproje</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

## Legacy QID Mappings

160611 Oracle Enterprise Linux Security Update for wireshark (ELSA-2023-2373)
184774 Debian Security Update for wireshark (CVE-2022-3190)
241420 Red Hat Update for wireshark (RHSA-2023:2373)
283520 Fedora Security Update for wireshark (FEDORA-2022-1f2fb087e)
283521 Fedora Security Update for wireshark (FEDORA-2022-9d4aa8a486)
296086 Oracle Solaris 11.4 Support Repository Update (SRU) 51.132.1 Missing (CPUOCT2022)
354316 Amazon Linux Security Advisory for wireshark : ALAS2022-2022-244
354561 Amazon Linux Security Advisory for wireshark : ALAS-2022-244
355161 Amazon Linux Security Advisory for wireshark : ALAS2023-2023-038
502965 Alpine Linux Security Update for wireshark
505831 Alpine Linux Security Update for wireshark
752600 SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2022:3309-1)
903889 Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (10920)
904416 Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (10920-1)
941027 AlmaLinux Security Update for wireshark (ALSA-2023:2373)

© [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](#).

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