



CVE-2021-39926

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-39926
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-19 17:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	Buffer overflow in the Bluetooth HCI_ISO dissector in Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection c

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	L
Heap-buffer-overflow in dissect_bthci_iso at packet-bthci_iso.c (#17649) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	g
[SECURITY] Fedora 34 Update: wireshark-3.6.0-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	li
Wireshark · wnpa-sec-2021-08 · Bluetooth HCI_ISO dissector crash	MISC	v
Debian -- Security Information -- DSA-5019-1 wireshark	DEBIAN	v
[SECURITY] Fedora 34 Update: wireshark-3.6.0-1.fc34 - package-announce - Fedora Mailing-Lists		li
Wireshark: Multiple Vulnerabilities (GLSA 202210-04) — Gentoo security	GENTOO	s
2021/CVE-2021-39926.json · master · GitLab.org / cves · GitLab	CONFIRM	g
[SECURITY] Fedora 35 Update: wireshark-3.6.0-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	li
[SECURITY] Fedora 35 Update: wireshark-3.6.0-1.fc35 - package-announce - Fedora Mailing-Lists		li

Vendor Comments And Credit

Discovery Credit

LEGACY: Doneing

Legacy QID Mappings

178933	Debian Security Update for wireshark (DSA 5019-1)
182368	Debian Security Update for wireshark (CVE-2021-39926)
282092	Fedora Security Update for wireshark (FEDORA-2021-97bd631e0a)
282134	Fedora Security Update for wireshark (FEDORA-2021-3747cf6107)
354338	Amazon Linux Security Advisory for wireshark : ALAS2022-2022-079
354457	Amazon Linux Security Advisory for wireshark : ALAS2022-2022-226
354540	Amazon Linux Security Advisory for wireshark : ALAS-2022-226
355161	Amazon Linux Security Advisory for wireshark : ALAS2023-2023-038
376111	Wireshark Bluetooth HCI_ISO Dissector Crash Vulnerability (wnpa-sec-2021-08)
502201	Alpine Linux Security Update for wireshark
502401	Alpine Linux Security Update for wireshark
710636	Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202210-04)
751469	OpenSUSE Security Update for wireshark (openSUSE-SU-2021:3938-1)
751516	OpenSUSE Security Update for wireshark (openSUSE-SU-2021:1566-1)
901756	Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7414)
902292	Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7414-1)

© 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](#)