



CVE-2022-32293

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

Summary

CVE	CVE-2022-32293
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-03 14:15:00 UTC
Updated	2023-12-21 18:51:00 UTC
Description	In ConnMan through 1.41, a man-in-the-middle attack against a WISPR HTTP query could be used to trigger a use-after-free

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Intel	Connman	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-5231-1 connman	DEBIAN	www.debian.org	
Bug 1200190 – VUL-0: CVE-2022-32293: connman: Double-free/Use-after-free in WISPR	CONFIRM	bugzilla.suse.com	
[PATCH 1/6] wispr: Rename wispr_portal_list to wispr_portal_hash - Daniel Wagner		lore.kernel.org	
[PATCH 3/6] wispr: Add reference counter to portal context - Daniel Wagner	CONFIRM	lore.kernel.org	
ConnMan: Multiple Vulnerabilities (GLSA 202310-21) — Gentoo security	GENTOO	security.gentoo.org	
[PATCH 1/6] wispr: Rename wispr_portal_list to wispr_portal_hash - Daniel Wagner	MISC	lore.kernel.org	
[PATCH 3/6] wispr: Add reference counter to portal context - Daniel Wagner		lore.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181049](#) Debian Security Update for connman (DLA 3105-1)

[181062](#) Debian Security Update for connman (DSA 5231-1)

[181121](#) Debian Security Update for connman (DLA 3144-1)

[183942](#) Debian Security Update for connman (CVE-2022-32293)

[199592](#) Ubuntu Security Notification for ConnMan Vulnerabilities (USN-6236-1)

[710781](#) Gentoo Linux ConnMan Multiple Vulnerabilities (GLSA 202310-21)

© [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](#)