



CVE-2023-32570

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

Summary

CVE	CVE-2023-32570
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-10 05:15:00 UTC
Updated	2023-11-07 04:14:00 UTC
Description	VideoLAN dav1d before 1.2.0 has a thread_task.c race condition that can lead to an application crash, related to dav1d_de

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Videolan	Dav1d	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 38 Update: dav1d-1.2.1-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
[SECURITY] Fedora 38 Update: dav1d-1.2.1-1.fc38 - package-announce - Fedora Mailing-Lists		lists.fedor
[SECURITY] Fedora 37 Update: dav1d-1.2.1-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedor
[SECURITY] Fedora 37 Update: dav1d-1.2.1-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
threading: Ensure passing the correct retval to decode_frame_exit (cf617fda) · Commits · VideoLAN / dav1d · GitLab	MISC	code.vide
1.2.0 · Tags · VideoLAN / dav1d · GitLab	MISC	code.vide
dav1d: Denial of Service (GLSA 202310-05) — Gentoo security	GENTOO	security.g
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284047](#) Fedora Security Update for dav1d (FEDORA-2023-9ea5d6e289)

[284310](#) Fedora Security Update for dav1d (FEDORA-2023-652b6e8847)

[710768](#) Gentoo Linux dav1dDenial of Service (DoS) Vulnerability (GLSA 202310-05)

© [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](#)