



CVE-2023-45322

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

Summary

CVE	CVE-2023-45322
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-06 22:15:00 UTC
Updated	2023-11-07 04:21:00 UTC
Description	** DISPUTED ** libxml2 through 2.11.5 has a use-after-free that can only occur after a certain memory allocation fails. This

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlsoft	Libxml2	All	All	All	All

References

Reference	Source	Link
Inject random malloc failures when fuzzing (#344) · Issues · GNOME / libxml2 · GitLab	MISC	gitlab.gnome.org
oss-security - CVE-2023-45322: Use-after-free in libxml2 through 2.11.5	MLIST	www.openwall.com
Memory error: heap-use-after-free in xmllint (xmlUnlinkNode) (#583) · Issues · GNOME / libxml2 · GitLab	MISC	gitlab.gnome.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[356548](#) Amazon Linux Security Advisory for libxml2 : ALAS-2023-1874

[356585](#) Amazon Linux Security Advisory for libxml2 : ALAS2-2023-2321

[356622](#) Amazon Linux Security Advisory for libxml2 : ALAS2023-2023-411

356985 Amazon Linux Security Advisory for libxml2 : AL2012-2023-469
673494 EulerOS Security Update for libxml2 (EulerOS-SA-2023-3311)
673502 EulerOS Security Update for libxml2 (EulerOS-SA-2023-3278)
673544 EulerOS Security Update for libxml2 (EulerOS-SA-2024-1090)
673900 EulerOS Security Update for libxml2 (EulerOS-SA-2024-1066)
673938 EulerOS Security Update for libxml2 (EulerOS-SA-2023-3250)
674092 EulerOS Security Update for libxml2 (EulerOS-SA-2023-3343)
710860 Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 202402-11)
755280 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:4464-1)
755304 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:4505-1)
755305 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:4504-1)
755325 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:4537-1)
907521 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (31272-1)

© [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](#)