



# CVE-2023-28484

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

## Summary

<b>CVE</b>	CVE-2023-28484
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-24 21:15:00 UTC
<b>Updated</b>	2024-02-01 17:15:00 UTC
<b>Description</b>	In libxml2 before 2.10.4, parsing of certain invalid XSD schemas can lead to a NULL pointer dereference and subsequently

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

## References

Reference	Source	Link	Tags
January 2024 MySQL Cluster Vulnerabilities in NetApp Products   NetApp Product Security		<a href="https://security.netapp.com">security.netapp.com</a>	
libxml2 2.10.4 · GNOME / libxml2 · GitLab	MISC	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	
[SECURITY] [DLA 3405-1] libxml2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
April 2023 Libxml2 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
[CVE-2023-28484] Segfault When Parsing XSD (#491) · Issues · GNOME / libxml2 · GitLab	MISC	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

160833 Oracle Enterprise Linux Security Update for libxml2 (ELSA-2023-4349)

<a href="#">160854</a> Oracle Enterprise Linux Security Update for libxml2 (ELSA-2023-4529)
<a href="#">181745</a> Debian Security Update for libxml2 (DSA 5391-1)
<a href="#">181756</a> Debian Security Update for libxml2 (DLA 3405-1)
<a href="#">184060</a> Debian Security Update for libxml2 (CVE-2023-28484)
<a href="#">199299</a> Ubuntu Security Notification for libxml2 Vulnerabilities (USN-6028-1)
<a href="#">199399</a> Ubuntu Security Notification for libxml2 Vulnerabilities (USN-6028-2)
<a href="#">241894</a> Red Hat Update for libxml2 (RHSA-2023:4349)
<a href="#">241937</a> Red Hat Update for libxml2 (RHSA-2023:4529)
<a href="#">242753</a> Red Hat Update for libxml2 (RHSA-2024:0413)
<a href="#">283897</a> Fedora Security Update for libxml2 (FEDORA-2023-dae7cc20ac)
<a href="#">284181</a> Fedora Security Update for libxml2 (FEDORA-2023-a521b917c8)
<a href="#">330144</a> IBM AIX Denial of Service (DoS) Vulnerability in libxml2 (libxml2_advisory5)
<a href="#">354918</a> Amazon Linux Security Advisory for libxml2 : ALAS2-2023-2021
<a href="#">354929</a> Amazon Linux Security Advisory for libxml2 : ALAS-2023-1743
<a href="#">355233</a> Amazon Linux Security Advisory for libxml2 : ALAS2023-2023-163
<a href="#">378891</a> Alibaba Cloud Linux Security Update for libxml2 (ALINUX3-SA-2023:0111)
<a href="#">378948</a> Oracle Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (CPUOCT2023)
<a href="#">502742</a> Alpine Linux Security Update for libxml2
<a href="#">673079</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2194)
<a href="#">673196</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2316)
<a href="#">673204</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2336)
<a href="#">673245</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2360)
<a href="#">673257</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2386)
<a href="#">673478</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2696)
<a href="#">673540</a> EulerOS Security Update for libxml2 (EulerOS-SA-2023-2654)
<a href="#">691148</a> Free Berkeley Software Distribution (FreeBSD) Security Update for libxml2 (0bd7f07b-dc22-11ed-bf28-589cfc0f81b0)
<a href="#">710860</a> Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 202402-11)
<a href="#">753947</a> SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:2048-1)

<a href="#">753949</a> SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:2054-1)
<a href="#">754861</a> SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:3665-1)
<a href="#">907101</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (26281-1)
<a href="#">941200</a> AlmaLinux Security Update for libxml2 (ALSA-2023:4349)
<a href="#">941217</a> AlmaLinux Security Update for libxml2 (ALSA-2023:4529)
<a href="#">961030</a> Rocky Linux Security Update for libxml2 (RLSA-2023:4529)

© [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](#)**