# CVE-2022-40304

Published on: Not Yet Published

Last Modified on: 11/23/2022 06:32:00 PM UTC

## CVE-2022-40304

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

The following vulnerability was found:

An issue was discovered in libxml2 before 2.10.3. Certain invalid XML entity definitions can corrupt a hash table key, potentially leading to subsequent logic errors. In one case, a double-free can be provoked.

CVE-2022-40304 has been assigned by cve@mitre.org to track the vulnerability

## CVE References

| Description | Tags | Link |
|---|---|---|
| [CVE-2022-40304] Fix dict corruption caused by entity reference cycles (1b41ec4e) · Commits · GNOME / libxml2 · GitLab | gitlab.gnome.org text/html | MISC gitlab.gnome.org/GNOME/libxml2/-/commit/1b41ec4e9433b05bb0376be4725804c54ef1d80b |
| v2.10.3 · Tags · GNOME / libxml2 · GitLab | gitlab.gnome.org text/html | MISC gitlab.gnome.org/GNOME/libxml2/-/tags/v2.10.3 |
| Tags · GNOME / libxml2 · GitLab | gitlab.gnome.org text/html | MISC gitlab.gnome.org/GNOME/libxml2/-/tags |



## Related QID Numbers

181179 Debian Security Update for libxml2 (DLA 3172-1)

181192 Debian Security Update for libxml2 (DSA 5271-1)

283234 Fedora Security Update for libxml2 (FEDORA-2022-aeafd24818)

377762 Apple MacOS Ventura 13.0.1 Not Installed (HT213504)

502547 Alpine Linux Security Update for libxml2

610450 Apple iOS 16.1.1 and iPadOS 16.1.1 Security Update Missing

710675 Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 202210-39)

752695 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:3692-1)

752722 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:3717-1)

752764 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:3871-1)

There are no known software configurations (CPEs) currently associated with this CVE

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @OpenBSD_ports | ajacoutot@ modified textproc/libxml: SECURITY update to libxml-2.10.3 - [CVE-2022-40304] Fix dict corruption caused… twitter.com/i/web/status/1… | 2022-10-15 12:55:18 |
| @OpenBSD_ports | OPENBSD_7_2 ajacoutot@ modified textproc/libxml: SECURITY update to libxml-2.10.3 - [CVE-2022-40304] Fix dict corru… twitter.com/i/web/status/1… | 2022-10-15 12:55:19 |
| @OpenBSD_stable | OPENBSD_7_2 ajacoutot@ modified textproc/libxml: SECURITY update to libxml-2.10.3 - [CVE-2022-40304] Fix dict corru… twitter.com/i/web/status/1… | 2022-10-15 12:55:19 |
| @OpenBSD_ports | OPENBSD_7_1 ajacoutot@ changed textproc/libxml: Merge SECURITY fixes from upstream: - [CVE-2022-40304] Fix dict cor… twitter.com/i/web/status/1… | 2022-10-15 12:55:20 |
| @OpenBSD_stable | OPENBSD_7_1 ajacoutot@ changed textproc/libxml: Merge SECURITY fixes from upstream: - [CVE-2022-40304] Fix dict cor… twitter.com/i/web/status/1… | 2022-10-15 12:55:21 |
| @autumn_good_35 | CVE-2022-37434 CVE-2022-40303 CVE-2022-40304 ClamAV® blog: New packages for ClamAV 0.103.7, 0.104.4, 0.105.1 to res… twitter.com/i/web/status/1… | 2022-11-01 15:09:30 |
| @0xdea | [CVE-2022-40304] Double-free when parsing default attributes // by @NedWilliamson gitlab.gnome.org/GNOME/libxml2/… | 2022-11-10 06:14:41 |
| @the_yellow_fall | CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… #opensource #infosec #security #pentesting | 2022-11-11 06:54:54 |
| @AcooEdi | CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS dlvr.it/ScbFD0 via securityonline https://t.co/pn5R9O4Aoy | 2022-11-11 06:58:35 |
| @lucianot54 | "CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS" via Penetration Testing ift.tt/6pKoB2S | 2022-11-11 07:17:18 |
| @FilipiPires | CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS ift.tt/q1FI2sD #security #opensource… twitter.com/i/web/status/1… | 2022-11-11 07:33:40 |
| @Dinosn | CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… | 2022-11-11 07:40:09 |
| @Komodosec | #Vulnerability #Apple CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… | 2022-11-11 11:05:32 |
| @PentestingN | CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… Penetration Testing CVE-20… twitter.com/i/web/status/1… | 2022-11-11 11:13:43 |
| @ernered | CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… #technology #feedly | 2022-11-13 16:05:38 |
| @hagieee | iOS/iPadOS 1.6.1.1リリース libxml2の脆弱性(CVE-2022-40303, CVE-2022-40304) 2件が修正 support.apple.com/ja-jp/HT213505 | 2022-11-14 04:48:10 |
| @jototsecnews | macOS / iOS のリモート・コード実行の脆弱性が FIX：CVE-2022-40303 / CVE-2022-40304 | 2022-11-19 |

| | | |
|---|---|---|
| @iototsecnews | macOS / iOS のリモートコード実行の脆弱性が FIX：CVE-2022-40303 / CVE-2022-40304 #security #apple #vulnerability iototsecnews.jp/2022/11/10/app… | 2022-11-19 22:08:46 |
| @CVEreport | CVE-2022-40304 : An issue was discovered in libxml2 before 2.10.3. Certain invalid XML entity definitions can corru… twitter.com/i/web/status/1… | 2022-11-23 18:05:41 |
| /r/k12cybersecurity | MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW | 2022-11-10 12:55:52 |
| /r/netcve | CVE-2022-40304 | 2022-11-23 18:38:35 |
| /r/DailyCVE | CVE-2022-40304 | 2022-11-23 20:16:08 |

← Previous ID

Next ID→