



Mozilla Firefox Use-After-Free Vulnerability

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-26485 |
| State | PUBLIC |
| Assigner | security@mozilla.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-12-22 20:15:00 UTC |
| Updated | 2022-12-30 16:22:00 UTC |
| Description | Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of a |

Risk And Classification

EPSS: 0.061260000 probability, percentile 0.907520000 (date 2026-04-01)

CISA KEV: Listed on 2022-03-07; due 2022-03-21; ransomware use Unknown

Problem Types: CWE-416

CISA Known Exploited Vulnerability

| | |
|------------------------|---|
| Vendor | Mozilla |
| Product | Firefox |
| Name | Mozilla Firefox Use-After-Free Vulnerability |
| Required Action | Apply updates per vendor instructions. |
| Notes | https://nvd.nist.gov/vuln/detail/CVE-2022-26485 |

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-------------------------|-------------------------------|---------|--------|---------|----------|
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Firefox Esr | All | All | All | All |
| Application | Mozilla | Firefox Focus | All | All | All | All |
| Application | Mozilla | Thunderbird | All | All | All | All |

References

| Reference | Source |
|-----------|--------|
|-----------|--------|

| | |
|--|---------|
| 1758062 - (CVE-2022-26485) heap-use-after-free txMozillaXSLTPProcessor.cpp:1361 in txVariable::Convert [exploited in the wild] | MISC |
| Security Vulnerabilities fixed in Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3.0, and Focus 97.3.0 — Mozilla | MISC |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |
| CISA Known Exploited Vulnerabilities catalog | CISA |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|---|
| 159696 Oracle Enterprise Linux Security Update for firefox (ELSA-2022-0824) |
| 159697 Oracle Enterprise Linux Security Update for firefox (ELSA-2022-0818) |
| 159705 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2022-0845) |
| 159706 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2022-0850) |
| 179101 Debian Security Update for firefox-esr (DSA 5090-1) |
| 179106 Debian Security Update for firefox-esr (DLA 2933-1) |
| 179108 Debian Security Update for firefox-esr (DLA 2933-1) |
| 179113 Debian Security Update for thunderbird (DSA 5094-1) |
| 179120 Debian Security Update for thunderbird (DLA 2939-1) |
| 184408 Debian Security Update for firefox-esrthunderbird (CVE-2022-26485) |
| 198689 Ubuntu Security Notification for Firefox Vulnerabilities (USN-5314-1) |
| 240124 Red Hat Update for firefox (RHSA-2022:0817) |
| 240132 Red Hat Update for firefox (RHSA-2022:0824) |
| 240133 Red Hat Update for firefox (RHSA-2022:0818) |
| 240136 Red Hat Update for firefox (RHSA-2022:0816) |
| 240141 Red Hat Update for thunderbird (RHSA-2022:0853) |
| 240142 Red Hat Update for thunderbird (RHSA-2022:0845) |
| 240143 Red Hat Update for thunderbird (RHSA-2022:0843) |
| 240145 Red Hat Update for thunderbird (RHSA-2022:0850) |
| 240433 Red Hat Update for thunderbird (RHSA-2022:0847) |
| 257161 CentOS Security Update for firefox (CESA-2022:0824) |

| |
|---|
| 257164 CentOS Security Update for thunderbird (CESA-2022:0850) |
| 282467 Fedora Security Update for firefox (FEDORA-2022-4f28c7541d) |
| 296057 Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (bulletinapr2022) |
| 353262 Amazon Linux Security Advisory for thunderbird : ALAS2-2022-1779 |
| 376447 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-09) |
| 376448 Mozilla Firefox ESR Multiple Vulnerabilities (MFSA2022-09) |
| 502074 Alpine Linux Security Update for firefox-esr |
| 502386 Alpine Linux Security Update for thunderbird |
| 502689 Alpine Linux Security Update for firefox |
| 504817 Alpine Linux Security Update for firefox-esr |
| 504827 Alpine Linux Security Update for firefox |
| 505453 Alpine Linux Security Update for thunderbird |
| 630848 Firefox For Android Use After Free Vulnerability |
| 630849 For ios Vulnerability CVE-2022-26485 |
| 710582 Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 202208-08) |
| 710585 Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 202208-14) |
| 751839 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2022:0777-1) |
| 751840 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2022:0783-1) |
| 751843 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2022:0778-1) |
| 751847 OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2022:0783-1) |
| 751857 OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2022:0804-1) |
| 753174 SUSE Enterprise Linux Security Update for MozillaThunderbird (SUSE-SU-2022:0804-1) |
| 753414 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2022:14906-1) |
| 940460 AlmaLinux Security Update for firefox (ALSA-2022:0818) |
| 940465 AlmaLinux Security Update for thunderbird (ALSA-2022:0845) |
| 960832 Rocky Linux Security Update for thunderbird (RLSA-2022:0845) |
| 960834 Rocky Linux Security Update for firefox (RLSA-2022:0818) |

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](#)