



CVE-2023-5724

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-5724 |
| State | PUBLIC |
| Assigner | security@mozilla.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-25 18:17:00 UTC |
| Updated | 2023-11-02 20:17:00 UTC |
| Description | Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This |

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 11.0 | All | All | All |
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Firefox ESR | All | All | All | All |
| Application | Mozilla | Thunderbird | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|--------------------------------------|-----------|
| [SECURITY] [DLA 3637-1] thunderbird security update | MISC | lists.debian.org | |
| Debian -- Security Information -- DSA-5535-1 firefox-esr | MISC | www.debian.org | |
| Security Vulnerabilities fixed in Firefox ESR 115.4 — Mozilla | MISC | www.mozilla.org | |
| Security Vulnerabilities fixed in Thunderbird 115.4.1 — Mozilla | MISC | www.mozilla.org | |
| [SECURITY] [DLA 3632-1] firefox-esr security update | MISC | lists.debian.org | |
| Access Denied | MISC | bugzilla.mozilla.org | |
| Debian -- Security Information -- DSA-5538-1 thunderbird | MISC | www.debian.org | |
| Security Vulnerabilities fixed in Firefox 119 — Mozilla | MISC | www.mozilla.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 161029 Oracle Enterprise Linux Security Update for firefox (ELSA-2023-6162) |
| 161033 Oracle Enterprise Linux Security Update for firefox (ELSA-2023-6187) |
| 161034 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2023-6191) |
| 161035 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2023-6194) |
| 161036 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2023-6193) |
| 161037 Oracle Enterprise Linux Security Update for firefox (ELSA-2023-6188) |
| 199869 Ubuntu Security Notification for Firefox Vulnerabilities (USN-6456-1) |
| 199889 Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-6468-1) |
| 242247 Red Hat Update for firefox (RHSA-2023:6162) |
| 242249 Red Hat Update for thunderbird (RHSA-2023:6198) |
| 242250 Red Hat Update for firefox (RHSA-2023:6189) |
| 242251 Red Hat Update for thunderbird (RHSA-2023:6197) |
| 242253 Red Hat Update for firefox (RHSA-2023:6188) |
| 242254 Red Hat Update for firefox (RHSA-2023:6186) |
| 242255 Red Hat Update for firefox (RHSA-2023:6185) |
| 242257 Red Hat Update for thunderbird (RHSA-2023:6196) |
| 242258 Red Hat Update for firefox (RHSA-2023:6199) |
| 242259 Red Hat Update for thunderbird (RHSA-2023:6195) |
| 242355 Red Hat Update for thunderbird (RHSA-2023:6194) |
| 242368 Red Hat Update for firefox (RHSA-2023:6187) |
| 242397 Red Hat Update for thunderbird (RHSA-2023:6191) |
| 296106 Oracle Solaris 11.4 Support Repository Update (SRU) 64.157.2 Missing (CPUOCT2023) |
| 356733 Amazon Linux Security Advisory for thunderbird : ALAS2-2023-2334 |
| 356892 Amazon Linux Security Advisory for firefox : ALAS2FIREFOX-2023-017 |
| 378958 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-45) |

| |
|---|
| 378959 Mozilla Firefox ESR Multiple Vulnerabilities (MFSA2023-46) |
| 378967 Mozilla Thunderbird Multiple Vulnerabilities (MFSA2023-47) |
| 503464 Alpine Linux Security Update for firefox |
| 503465 Alpine Linux Security Update for thunderbird |
| 505736 Alpine Linux Security Update for firefox-esr |
| 506072 Alpine Linux Security Update for firefox-esr |
| 506074 Alpine Linux Security Update for firefox |
| 506259 Alpine Linux Security Update for thunderbird |
| 6000256 Debian Security Update for firefox-esr (DLA 3632-1) |
| 6000286 Debian Security Update for thunderbird (DLA 3637-1) |
| 6000307 Debian Security Update for firefox-esr (DSA 5535-1) |
| 6000313 Debian Security Update for thunderbird (DSA 5538-1) |
| 710875 Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 202402-25) |
| 755161 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2023:4214-1) |
| 755162 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2023:4213-1) |
| 755163 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2023:4212-1) |
| 755199 SUSE Enterprise Linux Security Update for MozillaThunderbird (SUSE-SU-2023:4302-1) |
| 941333 AlmaLinux Security Update for thunderbird (ALSA-2023:6191) |
| 941334 AlmaLinux Security Update for firefox (ALSA-2023:6188) |
| 941341 AlmaLinux Security Update for firefox (ALSA-2023:6187) |
| 941343 AlmaLinux Security Update for thunderbird (ALSA-2023:6194) |
| 961069 Rocky Linux Security Update for firefox (RLSA-2023:6188) |

© [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](#)