



CVE-2021-43541

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-43541 |
| State | PUBLIC |
| Assigner | security@mozilla.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-12-08 22:15:00 UTC |
| Updated | 2022-12-09 15:59:00 UTC |
| Description | When invoking protocol handlers for external protocols, a supplied parameter URL containing spaces was not properly esc |

Risk And Classification

Problem Types: NVD-CWE-Other

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 |
| Operating System | Debian | Debian Linux | 9.0 | 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 |
|--|--------|--|------|
| Debian -- Security Information -- DSA-5026-1 firefox-esr | DEBIAN | www.debian.org | |
| Mozilla Thunderbird: Multiple Vulnerabilities (GLSA 202208-14) — Gentoo security | GENTOO | security.gentoo.org | |
| Security Vulnerabilities fixed in Thunderbird 91.4.0 — Mozilla | MISC | www.mozilla.org | |
| Mozilla Firefox: Multiple vulnerabilities (GLSA 202202-03) — Gentoo security | GENTOO | security.gentoo.org | |
| Debian -- Security Information -- DSA-5034-1 thunderbird | DEBIAN | www.debian.org | |
| Security Vulnerabilities fixed in Firefox 95 — Mozilla | MISC | www.mozilla.org | |
| Security Vulnerabilities fixed in Firefox ESR 91.4.0 — Mozilla | MISC | www.mozilla.org | |
| [SECURITY] [DLA 2863-1] firefox-esr security update | MLIST | lists.debian.org | |

| | | | |
|---|---------|---|---------------------|
| Access Denied | MISC | bugzilla.mozilla.org | |
| [SECURITY] [DLA 2874-1] thunderbird security update | MLIST | lists.debian.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 159547 Oracle Enterprise Linux Security Update for firefox (ELSA-2021-5013) |
| 159548 Oracle Enterprise Linux Security Update for firefox (ELSA-2021-5014) |
| 159549 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2021-5045) |
| 159550 Oracle Enterprise Linux Security Update for thunderbird (ELSA-2021-5046) |
| 178948 Debian Security Update for firefox-esr (DSA 5026-1) |
| 178970 Debian Security Update for firefox-esr (DLA 2863-1) |
| 178983 Debian Security Update for thunderbird (DSA 5034-1) |
| 178986 Debian Security Update for thunderbird (DLA 2874-1) |
| 179753 Debian Security Update for firefox-esr (CVE-2021-43541) |
| 198601 Ubuntu Security Notification for Firefox Vulnerabilities (USN-5186-1) |
| 198641 Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-5248-1) |
| 198643 Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-5246-1) |
| 239932 Red Hat Update for firefox (RHSA-2021:5014) |
| 239933 Red Hat Update for firefox (RHSA-2021:5016) |
| 239934 Red Hat Update for firefox (RHSA-2021:5015) |
| 239936 Red Hat Update for firefox (RHSA-2021:5013) |
| 239938 Red Hat Update for thunderbird (RHSA-2021:5046) |
| 239939 Red Hat Update for thunderbird (RHSA-2021:5048) |
| 239940 Red Hat Update for thunderbird (RHSA-2021:5045) |
| 239941 Red Hat Update for thunderbird (RHSA-2021:5047) |
| 257137 CentOS Security Update for firefox (CESA-2021:5014) |
| 376143 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-52) |

| |
|---|
| 376144 Mozilla Thunderbird Multiple Vulnerabilities (MFSA2021-54) |
| 376145 Mozilla Firefox ESR Multiple Vulnerabilities (MFSA2021-53) |
| 502071 Alpine Linux Security Update for firefox-esr |
| 502382 Alpine Linux Security Update for thunderbird |
| 502687 Alpine Linux Security Update for firefox |
| 505449 Alpine Linux Security Update for thunderbird |
| 710574 Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 202202-03) |
| 710585 Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 202208-14) |
| 751479 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2021:3995-1) |
| 751480 SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2021:4000-1) |
| 751510 OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2021:1575-1) |
| 751515 OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2021:3993-1) |
| 751542 OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2021:4150-1) |
| 751566 OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2021:1635-1) |
| 940263 AlmaLinux Security Update for firefox (ALSA-2021:5013) |
| 940397 AlmaLinux Security Update for thunderbird (ALSA-2021:5045) |
| 960845 Rocky Linux Security Update for firefox (RLSA-2021:5013) |
| 960881 Rocky Linux Security Update for thunderbird (RLSA-2021:5045) |

© [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](#)