



CVE-2023-6867

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

Summary

CVE	CVE-2023-6867
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-19 14:15:00 UTC
Updated	2024-02-02 02:35:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-1021

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	12.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All

References

Reference	Source	Link	Tags
lists.debian.org/debian-lts-announce/2023/12/msg00020.html		lists.debian.org	
www.debian.org/security/2023/dsa-5581		www.debian.org	Third Party Advisory
security.gentoo.org/glsa/202401-10		security.gentoo.org	
www.mozilla.org/security/advisories/mfsa2023-54		www.mozilla.org	Vendor Advisory
bugzilla.mozilla.org/show_bug.cgi		bugzilla.mozilla.org	Issue Tracking, Permissions Required
www.mozilla.org/security/advisories/mfsa2023-56		www.mozilla.org	Vendor Advisory
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

[161259](#) Oracle Enterprise Linux Security Update for firefox (ELSA-2024-0026)

[161262](#) Oracle Enterprise Linux Security Update for firefox (ELSA-2024-0025)

[161266](#) Oracle Enterprise Linux Security Update for firefox (ELSA-2024-0012)

[200019](#) Ubuntu Security Notification for Firefox Vulnerabilities (USN-6562-1)

[242639](#) Red Hat Update for firefox (RHSA-2024:0022)

[242640](#) Red Hat Update for firefox (RHSA-2024:0011)

[242641](#) Red Hat Update for firefox (RHSA-2024:0019)

[242642](#) Red Hat Update for firefox (RHSA-2024:0025)

[242645](#) Red Hat Update for firefox (RHSA-2024:0012)

[242646](#) Red Hat Update for firefox (RHSA-2024:0026)

[242653](#) Red Hat Update for firefox (RHSA-2024:0023)

[242655](#) Red Hat Update for firefox (RHSA-2024:0024)

[242661](#) Red Hat Update for firefox (RHSA-2024:0021)

[257291](#) CentOS Security Update for firefox (CESA-2024:0026)

[296108](#) Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)

[379170](#) Mozilla Firefox Multiple Vulnerabilities (MFSA2023-56)

[379171](#) Mozilla Firefox ESR Multiple Vulnerabilities (MFSA2023-54)

[510672](#) Alpine Linux Security Update for firefox-esr

[6000393](#) Debian Security Update for firefox-esr (DSA 5581-1)

[6000410](#) Debian Security Update for firefox-esr (DLA 3697-1)

[710830](#) Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 202401-10)

[755488](#) SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2023:4912-1)

[755509](#) SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2023:4929-1)

[755510](#) SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2023:4928-1)

[941514](#) AlmaLinux Security Update for firefox (ALSA-2024:0025)

[941517](#) AlmaLinux Security Update for firefox (ALSA-2024:0012)

© [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](#)