



CVE-2020-6805

Published on: 03/25/2020 12:00:00 AM UTC

Last Modified on: 02/10/2023 02:18:00 AM UTC

CVE-2020-6805

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

When removing data about an origin whose tab was recently closed, a use-after-free could occur in the Quota manager, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.

CVE-2020-6805 has been assigned by [m](#) security@mozilla.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [m](#) **Mozilla** - **Thunderbird** version < 68.6

Affected Vendor/Software: [m](#) **Mozilla** - **Firefox** version < 74

Affected Vendor/Software: [m](#) **Mozilla** - **Firefox** version < ESR68.6

Affected Vendor/Software: [m](#) **Mozilla** - **Firefox ESR** version < 68.6

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Vulnerabilities fixed in Firefox ESR 68.6 — Mozilla	Vendor Advisory www.mozilla.org text/html	 MISC www.mozilla.org/security/advisories/mfsa2020-09/
Security Vulnerabilities fixed in Firefox 74 — Mozilla	Vendor Advisory www.mozilla.org text/html	 MISC www.mozilla.org/security/advisories/mfsa2020-08/
USN-4328-1: Thunderbird vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4328-1
Security Vulnerabilities fixed in Thunderbird 68.6 — Mozilla	Vendor Advisory www.mozilla.org text/html	 MISC www.mozilla.org/security/advisories/mfsa2020-10/
USN-4335-1: Thunderbird vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-4335-1
1610880 - (CVE-2020-6805) heap-use-after-free (READ of size 8) in mozilla::dom::quota::QuotaObject::LockedMaybeUpdateSize	Issue Tracking Permissions Required bugzilla.mozilla.org text/html	 MISC bugzilla.mozilla.org/show_bug.cgi?id=1610880

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[178553](#) Debian Security Update for firefox-esr (DLA 2140-1)

[377015](#) Alibaba Cloud Linux Security Update for firefox (ALINUX2-SA-2020:0036)

[377080](#) Alibaba Cloud Linux Security Update for thunderbird (ALINUX2-SA-2020:0037)

[500927](#) Alpine Linux Security Update for firefox-esr

[500946](#) Alpine Linux Security Update for firefox

[501076](#) Alpine Linux Security Update for mozjs68

[502372](#) Alpine Linux Security Update for thunderbird

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Application	Mozilla	Firefox	All	All	All	All
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 Esr	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:						
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:						
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→