

Closed Bug 1915535 (CVE-2025-0238) Opened 1 year ago Closed 1 year ago

AddressSanitizer: heap-use-after-free on nsLineBreaker::FlushCurrentWord() after malloc failure

▼ Categories

Product: Core ▼

Component: Layout: Text and Fonts ▼

Type:  defect

Priority: P2 Severity: S2

▼ Tracking

Status: RESOLVED FIXED

Milestone: 135 Branch

Tracking Flags:

	Tracking	Status
firefox-esr115	134+	fixed
firefox-esr128	134+	fixed
firefox133	---	wontfix
firefox134	+	fixed
firefox135	+	fixed

► **People** (Reporter: sourc7, Assigned: jfkthame)

► **Details** (Keywords: csectype-uaf, reporter-external, sec-moderate, Whiteboard: [client-bounty-form][adv-main134+][adv-ESR128.6+][adv-ESR115.19+])

▼ Attachments

[minidump_0x838d084d.txt](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
9.15 KB, text/plain

[minidump_0x6573752d.txt](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
9.15 KB, text/plain

[minidump_sigill_0xebfdc845.txt](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
9.31 KB, text/plain

[nsLineBreaker-FlushCurrentWord.patch](#)

[Details](#) | [Diff](#) | [Splinter Review](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
738 bytes, patch

[testcase for patch.html](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
425 bytes, text/html

[log_ffp_asan_546144.log.552434.txt](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
22.29 KB, text/plain

Accept All Cookies

Reject All Non-Essential Cookies

[log_ffp_asan_1188513.log.1277779.txt](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
20.36 KB, text/plain

[minidump_esr115.txt](#)

[Details](#)

1 year ago [Irvan Kurniawan \[:sourc7\]](#)
6.08 KB, text/plain

[Bug 1915535 - Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=#layout](#)

[Details](#) | [Review](#)

1 year ago [Jonathan Kew \[:jfkthame\]](#)
48 bytes, text/x-phabricator-request

[Bug 1915535 - Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=#layout](#)

phab-bot : [approval-mozilla-beta+](#)

[Details](#) | [Review](#)

1 year ago [Jonathan Kew \[:jfkthame\]](#)
48 bytes, text/x-phabricator-request

[Bug 1915535 - Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=#layout](#)

phab-bot : [approval-mozilla-esr128+](#)

[Details](#) | [Review](#)

1 year ago [Jonathan Kew \[:jfkthame\]](#)
48 bytes, text/x-phabricator-request

[Bug 1915535 - \[esr115\] Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord.](#)

phab-bot : [approval-mozilla-esr115+](#)

[Details](#) | [Review](#)

1 year ago [Jonathan Kew \[:jfkthame\]](#)
48 bytes, text/x-phabricator-request

[advisory.txt](#)

[Details](#)

1 year ago [Frederik Braun \[:freddy\]](#)
194 bytes, text/plain

Bottom ↓

Tags ▼

Timeline ▼



[Irvan Kurniawan \[:sourc7\]](#)

Reporter

Description • 1 year ago

Attached file [minidump_0x838d084d.txt](#) — [Details](#)

Help us improve your Bugzilla@Mozilla experience

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.

After run `document.execCommand("insertLineBreak")` and `setRangeText` in loop, when malloc failure on `nsLineBreaker::FlushCurrentWord()` in `if (!breakState.AppendElements(length, mozilla::fallible)) {` Firefox able to crash with SIGSEGV/SEGV_ACCERR with changing address,

sometimes SIGILL/ILL_ILLOPN with changing top stack, and ASan heap-use-after-free on nsLineBreaker::FlushCurrentWord() with READ of size 4 (32-bit) and READ of size 8 (64-bit) ASan build

Tested on:

- Firefox 129.0.2 (32-bit)
- Firefox Nightly 131.0a1 (2024-08-28) (32-bit)

Steps to reproduce:

1. Apply attached nsLineBreaker-FlushCurrentWord.patch
2. Compile Firefox
3. Visit attached testcase.forpatch.html
4. Firefox crash with SIGSEGV / SEGV_ACCERR or AddressSanitizer: heap-use-after-free on ASan build

Flags: sec-bounty?

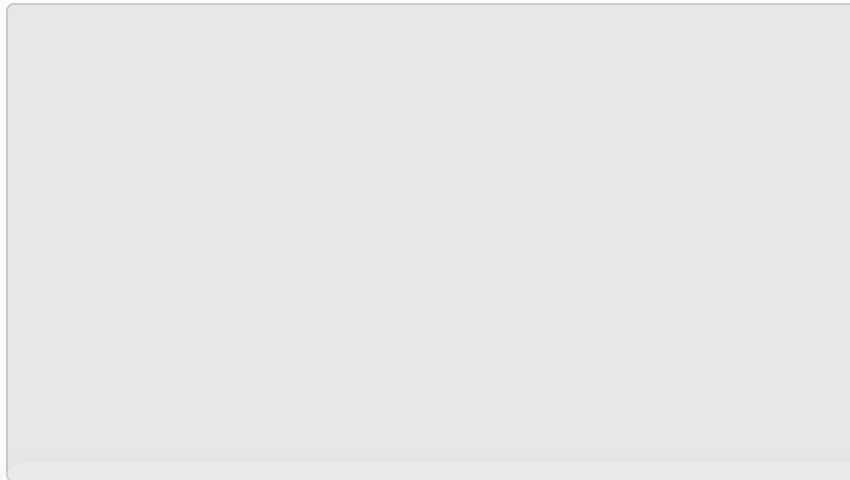


Irvan Kurniawan [:sourc7]

Reporter

Comment 1 • 1 year ago

Attached file [minidump_0x6573752d.txt](#) — [Details](#)



Irvan Kurniawan [:sourc7]

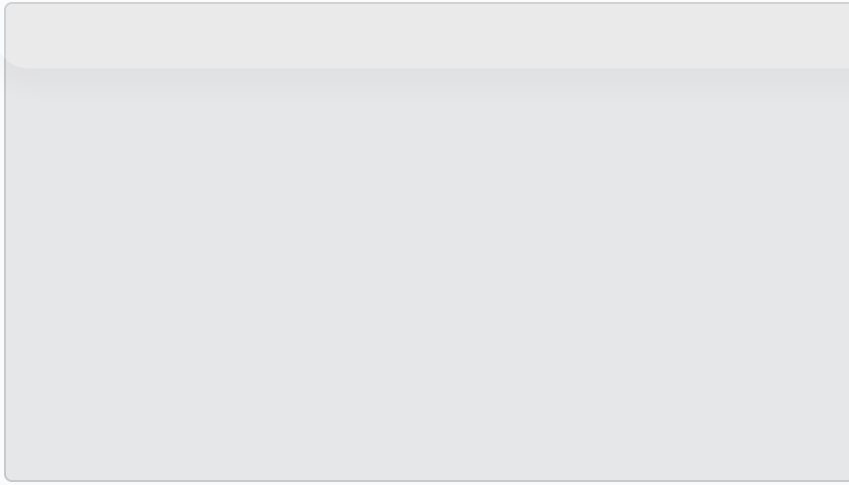
Reporter

Comment 2 • 1 year ago

Attached file [minidump_sigill_0xebfdc845.txt](#) — [Details](#)

Help us improve your Bugzilla@Mozilla experience

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.

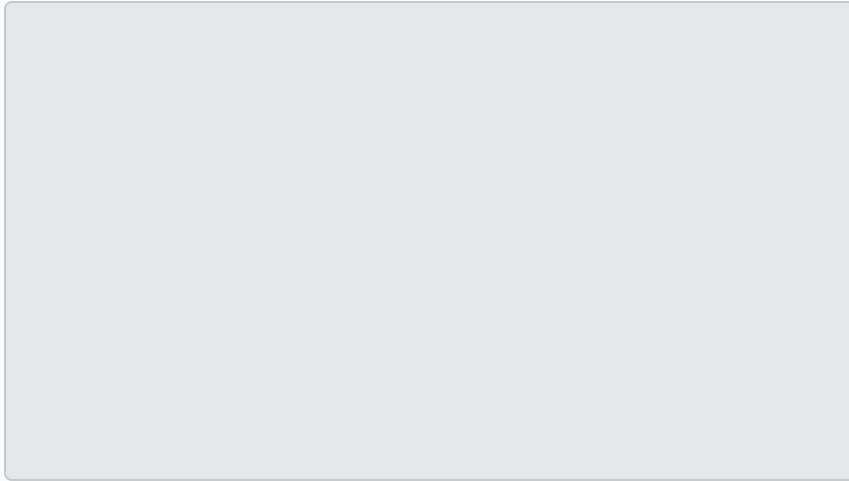


Irvan Kurniawan [:sourc7]

Reporter

Comment 3 • 1 year ago

Attached patch [nsLineBreaker-FlushCurrentWord.patch](#) — Details — Splinter Review



Irvan Kurniawan [:sourc7]

Reporter

Comment 4 • 1 year ago

Attached file [testcase.forpatch.html](#) — Details

Help us improve your Bugzilla@Mozilla experience

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.

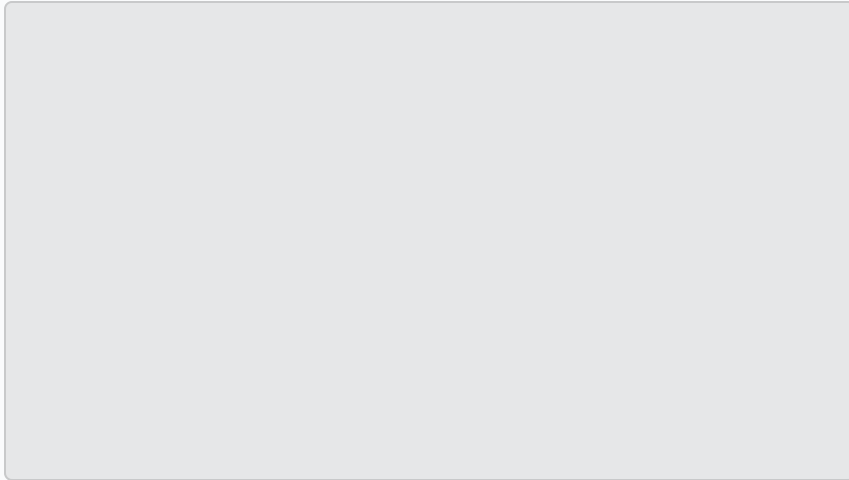


Irvan Kurniawan [:sourc7]

Reporter

Comment 5 • 1 year ago

Attached file [log_ffp_asan_546144.log.552434.txt](#) — Details

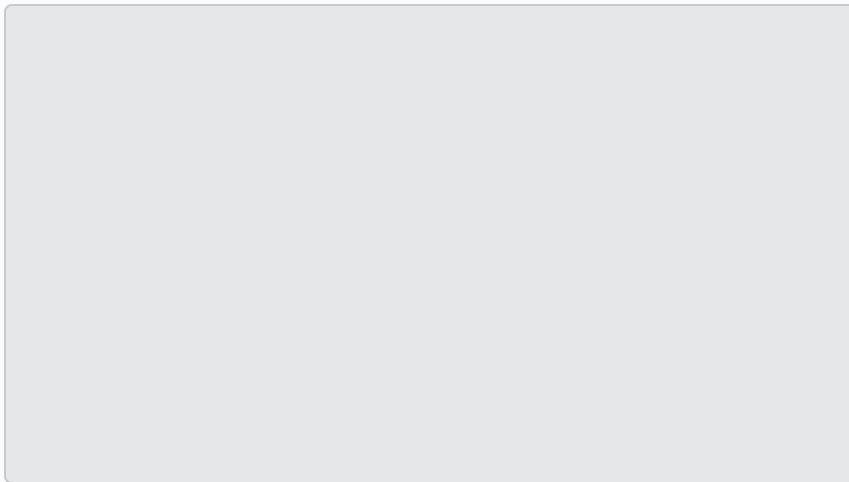


Irvan Kurniawan [:sourc7]

Reporter

Comment 6 • 1 year ago

Attached file [log_ffp_asan_1188513.log.1277779.txt](#) — Details



Andrew McCreight [:mccr8]

Comment 7 • 1 year ago

nsLineBreaker is under dom/ but it looks mostly related to text, so I'll put it in Layout.

I'm marking this sec-moderate because it requires an OOM. If you can demonstrate a reliable test case without patching Firefox, we could probably raise it to sec-high.

Group: firefox-core-security → layout-core-security

Component: Security → Layout: Text and Fonts

Keywords: [csectype-uaf](#), [sec-moderate](#)

Product: Firefox → Core

**Irvan Kurniawan [:sourc7]**

Reporter

Comment 8 • 1 year ago

(In reply to Andrew McCreight [:mccr8] from [comment #7](#))

I'm marking this sec-moderate because it requires an OOM. If you can demonstrate a reliable test case without patching Firefox, we could probably raise it to sec-high.

Thanks, I originally able to reproduce this on Firefox Nightly 32-bit official build, however the testcase is still intermittent, I'll try to improve the testcase reliability to hit SEGV_ACCERR crash.

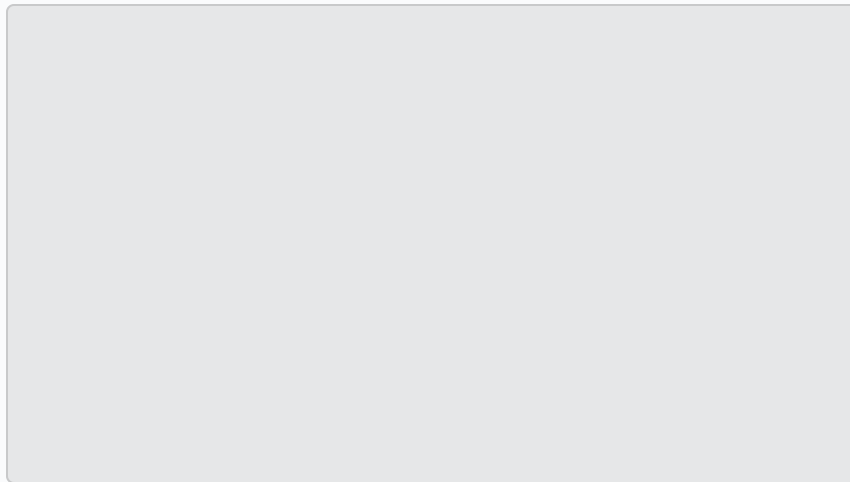
I also able to reproduce this on Firefox 115.14.0esr (32-bit).

**Irvan Kurniawan [:sourc7]**

Reporter

Comment 9 • 1 year ago

Attached file [minidump_esr115.txt](#) — [Details](#)

**Emilio Cobos Álvarez [:emilio]**

Comment 10 • 1 year ago

Let's start with S2, seems worth fixing.

Severity: -- → S2

Flags: needinfo?(jfkthame)

Priority: -- → P2

**Jonathan Kew [:jfkthame]**

Assignee

Comment 11 • 1 year ago


The problem here occurs because if we bail out of `FlushCurrentWord` due to an allocation failure (which could happen for either the `breakState` or `capitalizationState` arrays), we don't just fail to set up break positions and/or capitalization -- which is the expected result of the failure -- we also miss the final "cleanup" of state that's supposed to happen [at the end of `FlushCurrentWord`](#).

That doesn't *immediately* cause a problem, but it does leave the `mTextItems` array holding pointers that were supposed to be cleared, and are about to be freed. So then by the next time we call `FlushCurrentWord` those items are no longer valid, and we crash trying to access them.


The fix should be to ensure that we always clear the `mTextItems` array when `FlushCurrentWord` finishes, even if an error occurred so that we weren't able to set up breaks.

After doing that, the testcase here just happily infinite-loops, as expected. (Presumably it will eventually OOM in some other place, as it is endlessly adding content...)


Flags: needinfo?(jfkthame)

 **Jonathan Kew [jfkthame]** Assignee
Comment 12 • 1 year ago


Attached file [Bug 1915535 - Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=#layout](#) — Details

 **Phabricator Automation**
Updated • 1 year ago

Assignee: nobody → jfkthame
Status: NEW → ASSIGNED

 **Pulsebot**
Comment 13 • 1 year ago

Pushed by jkew@mozilla.com:
<https://hg.mozilla.org/integration/autoland/rev/10af4f9659db>
Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=layout-reviewers,emilio

 **Sebastian Hengst [aryx] (needinfo me if it's about an intermittent or backout)**
Comment 14 • 1 year ago • Edited

Backed out for non-unified build bustage on nsLineBreaker.cpp:
<https://hg.mozilla.org/integration/autoland/rev/03d28e6bd1f816bcdadef0f0f9de55af1dbdc6d>

[Help with failures](#)
[Build log](#)

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information to improve your Bugzilla@Mozilla experience. We value your privacy. You can manage your preferences at [https://bugzilla.mozilla.org/settings.html](#).

```
[task 2024-12-02T18:24:07.272Z] 18:24:07 ERROR - /builds/worker/checkouts/gecko/
[task 2024-12-02T18:24:07.273Z] 18:24:07 INFO - 154 | auto cleanup = MakeSc
[task 2024-12-02T18:24:07.274Z] 18:24:07 INFO - | ^~~~~~
[task 2024-12-02T18:24:07.274Z] 18:24:07 INFO - | mozilla
[task 2024-12-02T18:24:07.274Z] 18:24:07 INFO - /builds/worker/workspace/obj-bu
```

[task 2024-12-02T18:24:07.274Z] 18:24:07 INFO - 119 | [[nodiscard]] ScopeExit
[task 2024-12-02T18:24:07.274Z] 18:24:07 INFO - |



Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)

Updated • 1 year ago

Flags: needinfo?(jfkthame)



Jonathan Kew [:jfkthame] Assignee

Updated • 1 year ago

Flags: needinfo?(jfkthame)



Pulsebot

Comment 15 • 1 year ago

Pushed by jkew@mozilla.com:

<https://hg.mozilla.org/integration/autoland/rev/ac1f0158c2f2>

Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=layout-reviewers,emilio



Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)

Comment 16 • 1 year ago

<https://hg.mozilla.org/mozilla-central/rev/ac1f0158c2f2>

Group: layout-core-security → core-security-release

Status: ASSIGNED → RESOLVED

Closed: 1 year ago

status-firefox135: --- → fixed

Resolution: --- → FIXED

Target Milestone: --- → 135 Branch



Ryan VanderMeulen [:RyanVM]

Updated • 1 year ago

status-firefox133: --- → wontfix

status-firefox134: --- → affected

status-firefox-esr115: --- → affected

status-firefox-esr128: --- → affected

tracking-firefox134: --- → +

tracking-firefox135: --- → +

tracking-firefox-esr115: --- → 134+

tracking-firefox-esr128: --- → 134+



BugBot [:suhaib / :marco / :calixte]


Comment 17 • 1 year ago

The patch landed in nightly and beta is affected.
:jfkthame, is this bug important enough to require an uplift?

- If yes, please nominate the patch for beta approval.
- If no, please set `status-firefox134` to `wontfix`.


For more information, please visit [BugBot documentation](#).

Flags: needinfo?(jfkthame)

 **Jonathan Kew [:jfkthame]** Assignee
Comment 18 • 1 year ago

Attached file [Bug 1915535 - Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=#layout](#) — [Details](#)

Original Revision: <https://phabricator.services.mozilla.com/D230763>


 **Phabricator Automation**
Updated • 1 year ago

[Attachment #9441645](#) - Flags: approval-mozilla-beta?

 **Phabricator Automation**
Comment 19 • 1 year ago


beta Uplift Approval Request

- **User impact if declined:** potential use-after-free after a memory-allocation failure
- **Code covered by automated testing:** no
- **Fix verified in Nightly:** no
- **Needs manual QE test:** no
- **Steps to reproduce for manual QE testing:** n/a
- **Risk associated with taking this patch:** low
- **Explanation of risk level:** Just ensures early-return codepaths don't skip required cleanup
- **String changes made/needed:** none
- **Is Android affected?:** yes

 **Jonathan Kew [:jfkthame]** Assignee
Updated • 1 year ago

Flags: needinfo?(jfkthame)

In order for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.

 **Daniel Veditz [:dveditz]**
Updated • 1 year ago

Flags: sec-bounty? → sec-bounty+



Phabricator Automation

Updated • 1 year ago



Attachment #9441645 - Flags: approval-mozilla-beta? → approval-mozilla-beta+



Pulsebot

Comment 20 • 1 year ago



uplift

<https://hg.mozilla.org/releases/mozilla-beta/rev/53ea167def36>



Lando Automation

Updated • 1 year ago



status-firefox134: affected → fixed



Andrei Vaida [:avaida]

Updated • 1 year ago



QA Whiteboard: [post-critsmash-triage]
Flags: qe-verify-



Ryan VanderMeulen [:RyanVM]

Comment 21 • 1 year ago • Edited



Please nominate this for ESR128 and ESR115 approval. It'll need a minor bit of rebasing for ESR115.

Flags: needinfo?(jfkthame)



Jonathan Kew [:jfkthame]

Assignee

Comment 22 • 1 year ago



Attached file [Bug 1915535 - Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord. r=#layout](#) — Details

Original Revision: <https://phabricator.services.mozilla.com/D230763>



Phabricator Automation

Updated • 1 year ago



Attachment #9443207 - Flags: approval-mozilla-esr128?

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any other analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.

esr128 Uplift Approval Request

- **User impact if declined:** potential use-after-free after a memory-allocation failure
- **Code covered by automated testing:** no

- **Fix verified in Nightly:** no
- **Needs manual QE test:** no
- **Steps to reproduce for manual QE testing:** n/a
- **Risk associated with taking this patch:** low
- **Explanation of risk level:** Just ensures early-return codepaths don't skip required cleanup
- **String changes made/needed:** none
- **Is Android affected?:** yes



Jonathan Kew [jfkthame]

Assignee

Comment 24 • 1 year ago

Attached file [Bug 1915535 - \[esr115\] Ensure consistent cleanup in nsLineBreaker::FlushCurrentWord.](#) — Details



Phabricator Automation

Updated • 1 year ago

[Attachment #9443220](#) - Flags: approval-mozilla-esr115?



Phabricator Automation

Comment 25 • 1 year ago

esr115 Uplift Approval Request

- **User impact if declined:** potential use-after-free after a memory-allocation failure
- **Code covered by automated testing:** no
- **Fix verified in Nightly:** no
- **Needs manual QE test:** no
- **Steps to reproduce for manual QE testing:** n/a
- **Risk associated with taking this patch:** low
- **Explanation of risk level:** Just ensures early-return codepaths don't skip required cleanup
- **String changes made/needed:** none
- **Is Android affected?:** yes



Jonathan Kew [jfkthame]

Assignee

Updated • 1 year ago

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your Cookie Settings later.



Phabricator Automation

Updated • 1 year ago

[Attachment #9443220](#) - Flags: approval-mozilla-esr115? → approval-mozilla-esr115+

**Phabricator Automation**

Updated • 1 year ago

[Attachment #9443207](#) - Flags: approval-mozilla-esr128? → approval-mozilla-esr128+**Pulsebot**

Comment 26 • 1 year ago



uplift

<https://hg.mozilla.org/releases/mozilla-esr115/rev/1a28bb2e9696>**Lando Automation**

Updated • 1 year ago



status-firefox-esr115: affected → fixed

**Pulsebot**

Comment 27 • 1 year ago



uplift

<https://hg.mozilla.org/releases/mozilla-esr128/rev/29000f5f707e>**Lando Automation**

Updated • 1 year ago



status-firefox-esr128: affected → fixed

**Frederik Braun [:freddy]**

Updated • 1 year ago



Whiteboard: [client-bounty-form] → [client-bounty-form][adv-main134+][adv-ESR128.6+][adv-ESR115.19+]

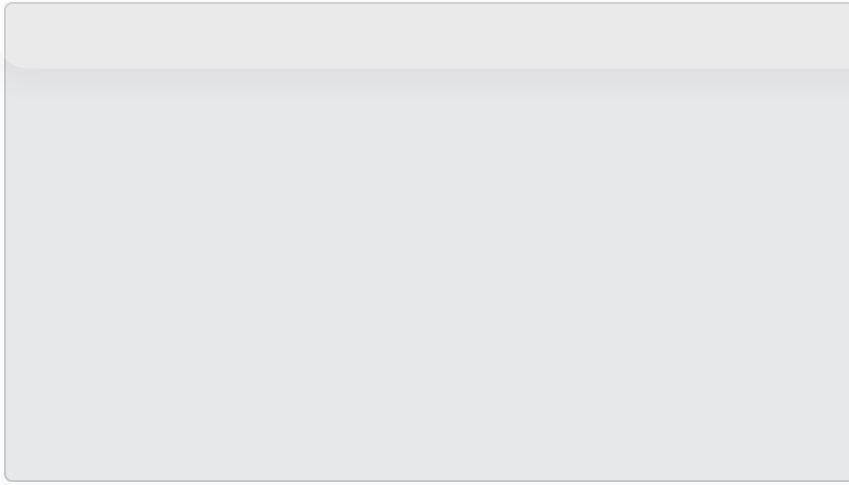
**Frederik Braun [:freddy]**

Comment 28 • 1 year ago

Attached file [advisory.txt](#) — [Details](#)

Help us improve your Bugzilla@Mozilla experience

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.



Frederik Braun [:freddy]

Updated • 1 year ago



Alias: CVE-2025-0238



Daniel Veditz [:dveditz]

Updated • 10 months ago



Group: ~~core-security-release~~

You need to [log in](#) before you can comment on or make changes to this bug.

Top ↑

Help us improve your Bugzilla@Mozilla experience

In addition to cookies necessary for this site to function, we'd like your permission to store some additional information that will improve your experience. Bugzilla does not use this information for tracking or any kind of analytics. Rest assured - we value your privacy. You will be able to change your [Cookie Settings](#) later.