Closed Bug 1936613 (CVE-2025-1009) Opened 1 year ago Closed 1 year ago

Firefox: use-after-free in txMozillaXSLTProcessor

Categories

Product: Core
Component: XSLT

Type: defect

Priority: *Not set* Severity: S2

Tracking

Status: VERIFIED FIXED

Milestone: 136 Branch

Tracking Flags:

	Tracking	Status
firefox-esr115	135+	verified
firefox-esr128	135+	verified
firefox133	---	wontfix
firefox134	---	wontfix
firefox135	+	verified
firefox136	+	verified

People (Reporter: ifratric, Assigned: mccr8)

References

Details (Keywords: csectype-uaf, reporter-external, sec-high, Whiteboard: [Disclosure deadline 2025-03-11][adv-main135+][adv-ESR115.20+][adv-ESR128.7+])

Attachments

xsltpoc.html Details
1 year ago **Ivan Fratric**
987 bytes, text/html

Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet. tjr : **sec-approval+** Details | Review
1 year ago **Andrew McCreight [:mccr8]**
48 bytes, text/x-phabricator-request

Bug 1936613 - Crash test. Details | Review
1 year ago **Andrew McCreight [:mccr8]**
48 bytes, text/x-phabricator-request

Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet. phab-bot : **approval-mozilla-beta+** Details | Review
1 year ago **Andrew McCreight [:mccr8]**
48 bytes, text/x-phabricator-request

Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet. phab-bot : **approval-mozilla-esr128+** Details | Review
1 year ago **Andrew McCreight [:mccr8]**
48 bytes, text/x-phabricator-request

Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet. phab-bot : **approval-mozilla-esr115+** Details | Review
1 year ago **Andrew McCreight [:mccr8]**
48 bytes, text/x-phabricator-request

advisory.txt Details
1 year ago **Tyson Smith [:tsmith]**
192 bytes, text/plain

Bottom ↓ Tags ▾ Timeline ▾

Multiple Authors
Description • 1 year ago • Edited

*Attached file **xsltpoc.html** — Details*

Steps to reproduce:

Please note:

This bug is subject to a 90-day disclosure deadline. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public at the deadline. The scheduled deadline is 2025-03-11.

For more details, see the Project Zero vulnerability disclosure policy:
https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-policy.html

For the discovery of this issue, please credit Tyson Smith of Google Project Zero.

There is a use-after-free vulnerability in Firefox in txMozillaXSLTProcessor. The vulnerability was reproduced with an ASAN build from the latest source code.
The PoC is attached. The correspondin ASAN log can be found at the end of this report. Root cause analysis follows.

txMozillaXSLTProcessor contains several fields that are relevant for understanding the vulnerability:

```
class txMozillaXSLTProcessor final : public nsIDocumentTransformer,
                                     public nsStubMutationObserver,
                                     public nsWrapperCache {
  ...
  RefPtr<txStylesheet> mStylesheet;
  mozilla::dom::Document* mStylesheetDocument;  // weak
  nsCOMPtr<nsIContent> mEmbeddedStylesheetRoot;
  ...
  nsresult mCompileResult;
};
```

mStylesheet is the compiled stylesheet, mStylesheetDocument is the document that contains the stylesheet and, if a node is passed to XSLTProcessor.importStylesheet rather than a document, then mEmbeddedStylesheetRoot contains a pointer to that node. mCompileResult contains the compilation result but is only set by some of the functions that perform compilation (we'll come back to that later).

Most notably, mStylesheetDocument is the raw pointer to the Document object. In order to prevent cases where the Document gets freed but is still referenced by txMozillaXSLTProcessor, txMozillaXSLTProcessor registers itself as a MutationObserver and implements the following function, which will be called before the document gets freed:

```
void txMozillaXSLTProcessor::NodeWillBeDestroyed(nsINode* aNode) {
  nsCOMPtr<nsIMutationObserver> kungFuDeathGrip(this);
  if (NS_FAILED(mCompileResult)) {
    return;
  }
  mCompileResult = ensureStylesheet();
  mStylesheetDocument = nullptr;
  mEmbeddedStylesheetRoot = nullptr;
}
```

As can be seen, before the document gets deleted, mStylesheetDocument gets set to nullptr. However, we only proceed to that point if not NS_FAILED(mCompileResult). And we can only set mCompileResult to failed from txMozillaXSLTProcessor::NodeWillBeDestroyed, at which point the mStylesheetDocument has already been set to nullptr.

But what if we can set mStylesheetDocument to *another* document *after* mCompileResult became FAILED. This would prevent the mutation observer from correctly executing for the second document.

Normally, we are not allowed to set mStylesheetDocument after it has been set previously. txMozillaXSLTProcessor::ImportStylesheet is meant to prevent that:

```
void txMozillaXSLTProcessor::ImportStylesheet(nsINode& aStyle,
                                              mozilla::ErrorResult& aRv) {
  // We don't support importing multiple stylesheets yet.
  if (NS_WARN_IF(mStylesheetDocument || mStylesheet)) {
    aRv.Throw(NS_ERROR_NOT_IMPLEMENTED);
    return;
  }
  ...
};
```

As can be seen, txMozillaXSLTProcessor::ImportStylesheet will fail if either mStylesheetDocument or mStylesheet are set. But we already saw that we can unset mStylesheetDocument in txMozillaXSLTProcessor::NodeWillBeDestroyed observer callback. And mStylesheet can also be unset by other observer callbacks, for example:

```
void txMozillaXSLTProcessor::ContentWillBeRemoved(nsIContent* aChild) {
  mStylesheet = nullptr;
}
```

So by using observer callbacks, we can get txMozillaXSLTProcessor to a state where both mStylesheetDocument and mStylesheet are NULL, but mCompileResult is FAILED.

Another hurdle to overcome before triggering the bug is that mCompileResult can only be set to FAILED during NodeWillBeDestroyed callback. But at this point, the document being destroyed is empty and the compilation of the empty document will actually succeed. To overcome this, we also set the mEmbeddedStylesheetRoot property (by calling txMozillaXSLTProcessor::ImportStylesheet on a node rather than a document), but we later detatch mEmbeddedStylesheetRoot from mStylesheetDocument using Document.adoptNode so that mStylesheetDocument could be freed (otherwise, mEmbeddedStylesheetRoot would hold a reference to mStylesheetDocument which would prevent freeing).

The entire exploit flow goes somewhat like this:

1. We call txMozillaXSLTProcessor::ImportStylesheet on a node. All of mStylesheet, mStylesheetDocument and mEmbeddedStylesheetRoot get set.
2. We detatch mEmbeddedStylesheetRoot from mStylesheetDocument by calling adoptNode on a different document.
3. We change the content of mEmbeddedStylesheetRoot so that compilation fails the next time. This also result in one of the observer callbacks setting mStylesheet to NULL.
4. We delete all other references to mStylesheetDocument. Garbage collector runs. txMozillaXSLTProcessor::NodeWillBeDestroyed runs. mCompileResult becomes FAILED, while mStylesheetDocument and mEmbeddedStylesheetRoot become NULL.
5. We call txMozillaXSLTProcessor::ImportStylesheet with a new document.

6. We drop all other references to the new document. txMozillaXSLTProcessor::NodeWillBeDestroyed runs but returns early due to NS_FAILED(mCompileResult). Document gets deleted and mStylesheetDocument points to freed memoy.
7. We call txMozillaXSLTProcessor::Reset. mStylesheetDocument->RemoveMutationObserver(this); is called with mStylesheetDocument being freed, resulting in a use-after-free.

ASAN log:

```
=================================================================
==766789==ERROR: AddressSanitizer: heap-use-after-free on address 0x51e0000180e0 at
READ of size 8 at 0x51e0000180e0 thread T0 (file:// Content)
    #0 0x7f0504a31b6d in GetExistingSlots firefox-source/dom/base/nsINode.h:2413:46
    #1 0x7f0504a31b6d in RemoveMutationObserver firefox-source/dom/base/nsINode.h:12
    #2 0x7f0504a31b6d in txMozillaXSLTProcessor::Reset() firefox-source/dom/xslt/xsl
    #3 0x7f04ff4b4fc8 in mozilla::dom::XSLTProcessor_Binding::reset(JSContext*, JS::
    #4 0x7f04ffe530ea in bool mozilla::dom::binding_detail::GenericMethod<mozilla::d
    #5 0x7f050783480f in CallJSNative firefox-source/js/src/vm/Interpreter.cpp:532:1
    #6 0x7f050783480f in js::InternalCallOrConstruct(JSContext*, JS::CallArgs const&
    #7 0x7f050784e27b in InternalCall firefox-source/js/src/vm/Interpreter.cpp:695:1
    #8 0x7f050784e27b in CallFromStack firefox-source/js/src/vm/Interpreter.cpp:700:
    #9 0x7f050784e27b in js::Interpret(JSContext*, js::RunState&) firefox-source/js/
    #10 0x7f05078335ce in MaybeEnterInterpreterTrampoline firefox-source/js/src/vm/I
    #11 0x7f05078335ce in js::RunScript(JSContext*, js::RunState&) firefox-source/js
    #12 0x7f050783878f in ExecuteKernel firefox-source/js/src/vm/Interpreter.cpp:893
    #13 0x7f050783878f in js::Execute(JSContext*, JS::Handle<JSScript*>, JS::Handle<
    #14 0x7f05079a5ba0 in ExecuteScript(JSContext*, JS::Handle<JSObject*>, JS::Handl
    #15 0x7f05079a5e60 in JS_ExecuteScript(JSContext*, JS::Handle<JSScript*>) firefo
    #16 0x7f0504c951c7 in ExecuteCompiledScript firefox-source/dom/script/ScriptLoad
    #17 0x7f0504c951c7 in mozilla::dom::ScriptLoader::EvaluateScript(nsIGlobalObject
    #18 0x7f0504c93f08 in mozilla::dom::ScriptLoader::EvaluateScriptElement(JS::load
    #19 0x7f0504c8c524 in mozilla::dom::ScriptLoader::ProcessRequest(JS::loader::Scr
    #20 0x7f0504c89523 in mozilla::dom::ScriptLoader::ProcessInlineScript(nsIScriptE
    #21 0x7f0504c71660 in mozilla::dom::ScriptLoader::ProcessScriptElement(nsIScript
    #22 0x7f0504c70f72 in mozilla::dom::ScriptElement::MaybeProcessScript() firefox-
    #23 0x7f04fb36fdc6 in AttemptToExecute firefox-source/objdir-ff-asan/dist/includ
```


Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Group: firefox-core-security → core-security
Component: Untriaged → XSLT
Product: Firefox → Core

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Group: core-security → dom-core-security
Flags: needinfo?(peterv)

Andrew McCreight [:mccr8] Assignee
Comment 1 • 1 year ago

I've updated the first comment to clean up the markup a little.

Daniel Veditz [:dveditz]
Updated • 1 year ago

Keywords: csectype-uaf, sec-high

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Severity: -- → S2

Andrew McCreight [:mccr8] Assignee
Comment 2 • 1 year ago

Attached file ***Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.*** — *Details*

Andrew McCreight [:mccr8] Assignee
Comment 3 • 1 year ago

The most obvious fix here is to change mStylesheetDocument to a WeakPtr. I confirmed that this patch stops the UAF. I don't know if we should address any of the other weird inconsistencies that the POC relies on.

At a glance, there are no other raw-pointer-as-weak-pointers in the XSLT implementation, or at least not any documented as such. We should really go through and try to get rid of all of them in DOM code...

Andrew McCreight [:mccr8] Assignee
Comment 4 • 1 year ago

Let's just fix the UAF here. Peter can look into the other weirdness described here if he wants later.

Assignee: nobody → continuation

Andrew McCreight [:mccr8] Assignee
Comment 5 • 1 year ago

Unfortunately this is not a full fix. I confirmed the fix when loading the test case independently. However, when I converted it to a crash test and ran it alongside the other XSLT crash tests, I hit another UAF.

We're in the `nsINode::LastRelease()` for a document and calling `NodeWillBeDestroyed`. I'm guessing the issue is that when we do the `adoptNode` and then the original document dies, the newly WeakPtr'd `mStylesheetDocument` safely turns into null. Hooray! But then in `~txMozillaXSLTProcessor()` this means we never call `RemoveMutationObserver`, so the new document has a dangling pointer. Oops. I guess I need to actually fix this issue on a deeper level.

Daniel Veditz [:dveditz]
Updated • 1 year ago

Keywords: reporter-external

Andrew McCreight [:mccr8] Assignee
Comment 6 • 1 year ago

The new UAF is actually in a different test `1527277.html`, which just hits an error. I suspect the problem is something like: Document gets unlinked (clearing the weak reference), txMozillaXSLTProcessor gets destroyed (weak ref is null, so it can't RemoveMutationObserver itself), Document gets destroyed (triggering the observer on the dead object). Back to the drawing board I guess.

Phabricator Automation
Updated • 1 year ago

Attachment #9443103 - Attachment description: Bug 1936613 - Use WeakPtr in txMozillaXSLTProcessor. → Bug 1936613 - Don't early return from txMozillaXSLTProcessor::NodeWillBeDestroyed.

Andrew McCreight [:mccr8] Assignee
Comment 7 • 1 year ago

Attached file ***Bug 1936613 - Crash test.*** *— Details*

Peter Van der Beken [:peterv]
Comment 8 • 1 year ago

Maybe `txMozillaXSLTProcessor::ImportStylesheet` can call `txMozillaXSLTProcessor::Reset` first? I'm not sure why `mStylesheetDocument` is weak though, but if the `Reset` thing works we might want to do that in a followup.

Flags: needinfo?(continuation)

Andrew McCreight [:mccr8] Assignee
Comment 9 • 1 year ago

Thanks for taking a look. I thought I tried making `mStylesheetDocument` and it leaked, but I tried it again now and I didn't see a leak. Maybe I forgot to make it CC'ed the first time? Anyways unfortunately making it strong causes browser_bug1309630.js to time out, though now I'm not seeing any leaks. I was

mostly avoiding it because it could cause a bunch of leakiness that might be hard to find. I'll try the reset thing.

Andrew McCreight [:mccr8] Assignee
Comment 10 • 1 year ago

Today is the last day for uplifts to beta 134, so given the uncertainty here, it'll have to wait until next release cycle. I think this dates to ~~bug 199331~~ which landed in 2003 so this can probably wait a few more weeks.

status-firefox133: --- → wontfix
status-firefox134: --- → wontfix
status-firefox135: --- → affected
status-firefox-esr115: --- → affected
status-firefox-esr128: --- → affected

Andrew McCreight [:mccr8] Assignee
Comment 11 • 1 year ago

(In reply to Peter Van der Beken [:peterv] from ~~comment #8~~)

> Maybe `txMozillaXSLTProcessor::ImportStylesheet` can call `txMozillaXSLTProcessor::Reset` first? I'm not sure why `mStylesheetDocument` is weak though, but if the `Reset` thing works we might want to do that in a followup.

That does seem to also fix the issue. Doesn't that change the behavior in the case where you do an import twice, though? Is that not a problem?

Flags: ~~needinfo?(continuation)~~

Andrew McCreight [:mccr8] Assignee
Comment 12 • 1 year ago

I also audited the other implementations of NodeWillBeDestroyed and I didn't notice any others that did this weird early return thing.

Peter Van der Beken [:peterv]
Comment 13 • 1 year ago

(In reply to Andrew McCreight [:mccr8] from ~~comment #11~~)

> That does seem to also fix the issue. Doesn't that change the behavior in the case where you do an import twice, though? Is that not a problem?

Hmm, I guess the main problem is that then the parameters/variables would also be cleared. I had an alternative approach in https://phabricator.services.mozilla.com/D231880#8036293, up to you.

Flags: ~~needinfo?(peterv)~~

Phabricator Automation
Updated • 1 year ago

Attachment #9443103 - Attachment description: Bug 1936613 - Don't early return from txMozillaXSLTProcessor::NodeWillBeDestroyed. → Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Blocks: ~~1937634~~

Andrew McCreight [:mccr8] Assignee
Comment 14 • 1 year ago

I filed ~~bug 1937634~~ about making this reference strong. The browser_bug1309630.js timeout I mentioned was a preexisting issue, but I'm still a little nervous about whether making it a strong ref will cause a leak.

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Whiteboard: [Disclosure deadline 2025-03-11]

Andrew McCreight [:mccr8] Assignee
Comment 15 • 1 year ago

Comment on attachment 9443103 [details]
~~Bug 1936613~~ - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.

Security Approval Request

- **How easily could an exploit be constructed based on the patch?**: The steps involved are a bit convoluted, but you might be able to work backwards to figure out how to cause the UAF. This bug is 21 years old AFAICT.
- **Do comments in the patch, the check-in comment, or tests included in the patch paint a bulls-eye on the security problem?**: No
- **Which branches (beta, release, and/or ESR) are affected by this flaw, and do the release status flags reflect this affected/unaffected state correctly?**: all
- **If not all supported branches, which bug introduced the flaw?**: None
- **Do you have backports for the affected branches?**: No
- **If not, how different, hard to create, and risky will they be?**: Shouldn't be an issue. This is a small, local fix to a file that doesn't change much.

- **How likely is this patch to cause regressions; how much testing does it need?**: Not likely. I don't think it'll affect behavior except in the case where the exploit is being triggered.
- **Is the patch ready to land after security approval is given?**: Yes
- **Is Android affected?**: Yes

Attachment #9443103 - Flags: sec-approval?

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

tracking-firefox135: --- → +
tracking-firefox-esr115: --- → 135+
tracking-firefox-esr128: --- → 135+

Tom Ritter [:tjr]
Comment 16 • 1 year ago

Comment on attachment 9443103 [details]
~~Bug 1936613~~ - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.

Approved to land and uplift

Attachment #9443103 - Flags: sec-approval? → sec-approval+

Tom Ritter [:tjr]
Updated • 1 year ago

Whiteboard: [Disclosure deadline 2025-03-11] → [Disclosure deadline 2025-03-11][reminder-test 2025-02-18]

Pulsebot
Comment 17 • 1 year ago

Pushed by amccreight@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/9d746bbe4f0a
Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet. r=peterv

Ryan VanderMeulen [:RyanVM]
Comment 18 • 1 year ago

https://hg.mozilla.org/mozilla-central/rev/9d746bbe4f0a

Group: dom-core-security → core-security-release
Status: NEW → RESOLVED
Closed: 1 year ago
status-firefox136: --- → fixed
tracking-firefox136: --- → +
Resolution: --- → FIXED

Target Milestone: --- → 136 Branch

BugBot [:suhaib / :marco/ :calixte]
Comment 19 • 1 year ago

The patch landed in nightly and beta is affected.
:mccr8, is this bug important enough to require an uplift?

- If yes, please nominate the patch for beta approval.
- If no, please set `status-firefox135` to `wontfix`.

For more information, please visit BugBot documentation.

Flags: needinfo?(continuation)

Andrew McCreight [:mccr8] Assignee
Comment 20 • 1 year ago

Attached file ***Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.*** — *Details*

Original Revision: https://phabricator.services.mozilla.com/D231880

Phabricator Automation
Updated • 1 year ago

Attachment #9446568 - Flags: approval-mozilla-beta?

Phabricator Automation
Comment 21 • 1 year ago

beta Uplift Approval Request

- **User impact if declined**: sec-high
- **Code covered by automated testing**: yes
- **Fix verified in Nightly**: yes
- **Needs manual QE test**: yes
- **Steps to reproduce for manual QE testing**: Load the xsltpoc.html attachment, see if it crashes after a few seconds
- **Risk associated with taking this patch**: low
- **Explanation of risk level**: this should only change the behavior in a weird case where we'd crash anyways
- **String changes made/needed**: none
- **Is Android affected?**: yes

Flags: qe-verify+

Andrew McCreight [:mccr8] Assignee
Comment 22 • 1 year ago

I checked that the attachment doesn't crash for me on MacOS Nightly, but it would still be good to have a real verification done.

Andrew McCreight [:mccr8] Assignee
Comment 23 • 1 year ago

Attached file ***Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.*** — *Details*

Original Revision: https://phabricator.services.mozilla.com/D231880

Phabricator Automation
Updated • 1 year ago

Attachment #9446571 - Flags: approval-mozilla-esr128?

Phabricator Automation
Comment 24 • 1 year ago

esr128 Uplift Approval Request

- **User impact if declined**: sec-high
- **Code covered by automated testing**: yes
- **Fix verified in Nightly**: yes
- **Needs manual QE test**: yes
- **Steps to reproduce for manual QE testing**: Load the xsltpoc.html attachment, see if it crashes after a few seconds
- **Risk associated with taking this patch**: low
- **Explanation of risk level**: this should only change the behavior in a weird case where we'd crash anyways
- **String changes made/needed**: none
- **Is Android affected?**: yes

Andrew McCreight [:mccr8] Assignee
Comment 25 • 1 year ago

Attached file ***Bug 1936613 - Reset mCompileResult in txMozillaXSLTProcessor::ImportStylesheet.*** — *Details*

Original Revision: https://phabricator.services.mozilla.com/D231880

Phabricator Automation
Updated • 1 year ago

Attachment #9446572 - Flags: approval-mozilla-esr115?

Phabricator Automation
Comment 26 • 1 year ago

esr115 Uplift Approval Request

- **User impact if declined**: sec-high
- **Code covered by automated testing**: yes
- **Fix verified in Nightly**: yes
- **Needs manual QE test**: yes
- **Steps to reproduce for manual QE testing**: Load the xsltpoc.html attachment, see if it crashes after a few seconds
- **Risk associated with taking this patch**: low
- **Explanation of risk level**: this should only change the behavior in a weird case where we'd crash anyways
- **String changes made/needed**: none
- **Is Android affected?**: yes

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Flags: ~~needinfo?(continuation)~~

Phabricator Automation
Updated • 1 year ago

Attachment #9446568 - Flags: approval-mozilla-beta? → approval-mozilla-beta+

Pulsebot
Comment 27 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-beta/rev/9258a5a83a4d

Lando Automation
Updated • 1 year ago

status-firefox135: affected → fixed

Andrei Vaida [:avaida]
Updated • 1 year ago

QA Whiteboard: [post-critsmash-triage]

Brindusa Tot, DTE
Updated • 1 year ago

QA Whiteboard: [post-critsmash-triage] → [post-critsmash-triage] [qa-triaged]

Phabricator Automation
Updated • 1 year ago

Attachment #9446571 - Flags: approval-mozilla-esr128? → approval-mozilla-esr128+

Phabricator Automation
Updated • 1 year ago

Attachment #9446572 - Flags: approval-mozilla-esr115? → approval-mozilla-esr115+

Pulsebot
Comment 28 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-esr128/rev/a381ae32d77a

Lando Automation
Updated • 1 year ago

status-firefox-esr128: affected → fixed

Pulsebot
Comment 29 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-esr115/rev/24caec54fd22

Lando Automation
Updated • 1 year ago

status-firefox-esr115: affected → fixed

Alexandru Trif, Desktop Test Engineering [atrif]
Comment 30 • 1 year ago • Edited

Reproduced the issue on Ubuntu 24.04. by following the next steps:

1. Download Firefox (2024-12-11) ASAN fuzzing build with fuzzfetch: `fuzzfetch -a --fuzzing --build 2024-12-11`
2. Run Grizzly replay with the `xsltpoc.html` testcase downloaded locally: `python3 -m grizzly.replay '/home/svuser/m-c-20241211100250-fuzzing-asan-opt/firefox' '/home/svuser/Downloads/xsltpoc.html'`

AR: Firefox closes and the Grizzly console reports `Result successfully reproduced: AddressSanitizer: heap-use-after-free [@ GetExistingSlots] with READ of size 8 (6386aab7:b9cb1e5b)`

The issue no longer occurs (no results detected) on Ubuntu 24.04 by following the above steps with ASAN fuzzing Firefox 136.0a1 (20250112212231), 135.0b4 (20250112225912), 128.7.0esr (20250112190713), 115.20.0esr (20250110165353- downloaded manually from link). If any further verification is needed, please let us know.

Status: RESOLVED → VERIFIED
status-firefox135: fixed → verified
status-firefox136: fixed → verified
status-firefox-esr115: fixed → verified
status-firefox-esr128: fixed → verified
Flags: ~~qe-verify+~~

Frederik Braun [:freddy]
Comment 31 • 1 year ago

Apropos of nothing, why is this patch adding debug assert and not a release assert?

Flags: needinfo?(continuation)

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Flags: needinfo?(continuation) → needinfo?(peterv)

Peter Van der Beken [:peterv]
Comment 32 • 1 year ago

Because `mEmbeddedStylesheetRoot` should be reset when `mStylesheet` is reset (which we do). Failing to do so would not be dramatic, it might lead to weird behaviour though. What exactly would you be worried about?

Flags: ~~needinfo?(peterv)~~

Peter Van der Beken [:peterv]
Updated • 1 year ago

Flags: needinfo?(freddy)

Frederik Braun [:freddy]
Comment 33 • 1 year ago

Not worried about anything in particular. It just caught my eye as odd from a high level, when a security patch is adding an assertion that isn't in release :)

Flags: ~~needinfo?(fbraun)~~

Tyson Smith [:tsmith]
Updated • 1 year ago

Whiteboard: [Disclosure deadline 2025-03-11][reminder-test 2025-02-18] → [Disclosure deadline 2025-03-11][reminder-test 2025-02-18][adv-main135+]

Tyson Smith [:tsmith]
Updated • 1 year ago

Whiteboard: [Disclosure deadline 2025-03-11][reminder-test 2025-02-18][adv-main135+] → [Disclosure deadline 2025-03-11][reminder-test 2025-02-18][adv-main135+][adv-ESR115.20+][adv-ESR128.7+]

Tyson Smith [:tsmith]
Comment 34 • 1 year ago

Attached file ***advisory.txt*** *— Details*

Frederik Braun [:freddy]
Updated • 1 year ago

Alias: CVE-2025-1009

BugBot [:suhaib / :marco/ :calixte]
Comment 35 • 1 year ago

a month ago, tjr placed a reminder on the bug using the whiteboard tag [reminder-test 2025-02-18].
mccr8, please refer to the original comment to better understand the reason for the reminder.

Flags: needinfo?(continuation)
Whiteboard: [Disclosure deadline 2025-03-11][reminder-test 2025-02-18][adv-main135+][adv-ESR115.20+][adv-ESR128.7+] → [Disclosure deadline 2025-03-11][adv-main135+][adv-ESR115.20+][adv-ESR128.7+]

Pulsebot
Comment 36 • 1 year ago

Pushed by amccreight@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/662368d56774
Crash test. r=smaug

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 37 • 1 year ago

https://hg.mozilla.org/mozilla-central/rev/662368d56774

Flags: in-testsuite+

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

Flags: ~~needinfo?(continuation)~~

Andrew McCreight [:mccr8] Assignee
Updated • 1 year ago

See Also: → https://project-zero.issues.chromium.org/issues/383558273

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 ↑