Closed Bug 1915257 (CVE-2025-0237) Opened 1 year ago Closed 1 year ago

WebChannel trusts the principal it gets from content for permission checking

Categories

Product: Toolkit
Component: General

Type: defect

Priority: P3 Severity: S4

Tracking

Status: RESOLVED FIXED
Milestone: 134 Branch

Tracking Flags:

	Tracking	Status
firefox-esr115	---	wontfix
firefox-esr128	134+	fixed
firefox132	---	wontfix
firefox133	---	wontfix
firefox134	+	fixed

People (Reporter: mccr8, Assigned: freddy)

References

Details (Keywords: csectype-priv-escalation, sec-moderate, sec-want, Whiteboard: [adv-main134+][adv-ESR128.6+])

Attachments

Bug 1915257 - POC for WebChannel check bypass (after content process takeover). WIP not for landing Details | Review
1 year ago **Andrew McCreight [:mccr8]**
48 bytes, text/x-phabricator-request

Bug 1915257 - refactor webchannel to use actor's principal r=nalexander RyanVM : **approval-mozilla-esr128+** Details | Review
1 year ago **Frederik Braun [:freddy]**
48 bytes, text/x-phabricator-request

advisory.txt Details
1 year ago **Frederik Braun [:freddy]**
288 bytes, text/plain

Bottom ↓ Tags Timeline

Andrew McCreight [:mccr8] Reporter
Description • 1 year ago

WebChannel is an actor that allows every webpage to send a `WebChannelMessageToChrome` message up to the parent process. Chrome JS in the parent process can register to receive these messages. A

message is only routed to the provided callback if the principal matches the one provided at registration time (or, similarly, the principal has a specified permission). However, this principal is not derived from the principal of the content process. Instead, the content process can pass whatever principal it wants. This means that if a hostile webpage has achieved arbitrary code execution in the content process then it can easily fake it.

I'm not sure how bad of a security problem this is. From what I can tell, there are 3 users of WebChannel:

1. Remote troubleshooting. If the principal in the message has the `remote-troubleshooting` permission (which by default only `https://support.mozilla.org/` has), it can request some data that is more or less like about:support, with a few things (crash ids, modified preferences, printing preferences) removed. The most sensitive data I could see was detailed hardware information, the installation directory, and the profile directory. This might be available to a compromised content process anyways through a few other means. Apparently this is still being used by Sumo, according to a Slack thread Gijs found from a few months ago.
2. The Gecko Profiler. This is limited to the principal `https://profiler.firefox.com` (well, or another one if you set a pref). GET_PROFILE looks a little iffy, in that you might be able to get a screenshot of other pages that are open. Probably not that bad. You can add a little profiler button to the Firefox UI which is funny and I use that in my demo but it doesn't seem bad exactly.
3. FxAccounts. This is potentially the scariest, but fortunately it looks like the code already does its own security check against data which is not supplied by the content process (`sendingContext.browsingContext`, which looks to originate from here in the parent process), so I think this should be okay.

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

*Attached file **Bug 1915257 - POC for WebChannel check bypass (after content process takeover). WIP not for landing** — Details*

Apply the patch, then load either:
file_web_channel.html?profiler
file_web_channel.html?remote-troubleshooting

The first will add the Profiler button to the UI.

The second will dump some information to the terminal console.
It also puts the data it got into window.theData so you can
poke at it with a debugger.

:Gijs (he/him)
Comment 2 • 1 year ago

Sounds like we should change https://searchfox.org/mozilla-central/rev/6ad5adeba2b4353c53fd3c714223becd78cda029/toolkit/actors/WebChannelParent.sys.mjs#31-37 to check the window global principal for the sender of the message, instead of a principal being passed?

Though I also wonder if there's a TOCTOU type issue here if the message is sent from a BC which is then immediately navigated...

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

A particular instance of a parent window actor is only associated with a single origin so I don't think navigation can cause an issue. (I double checked that with Nika, and hopefully I didn't not misunderstand her.)

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

See Also: → ~~1915280~~

Frederik Braun [:freddy] Assignee
Comment 4 • 1 year ago

(In reply to :Gijs (he/him) from ~~comment #2~~)

> Sounds like we should change https://searchfox.org/mozilla-central/rev/6ad5adeba2b4353c53fd3c714223becd78cda029/toolkit/actors/WebChannelParent.sys.mjs#31-37 to check the window global principal for the sender of the message, instead of a principal being passed?

Ideally, we wouldn't pass or receive any principal and just use the one from the window global for all subsequent checks.

Tom Ritter [:tjr]
Comment 5 • 1 year ago

This is all very related to the validated w2e added pre-fission for FxA and AMO - ~~Bug 1539595~~

See Also: → ~~CVE-2019-11741~~

Daniel Veditz [:dveditz]
Updated • 1 year ago

Keywords: csectype-priv-escalation, sec-moderate

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

Product: Firefox → Toolkit

Nick Alexander :nalexander [he/him]
Comment 6 • 1 year ago

I'm going to say this is P3 (Mozilla should fix it) and S4 (low severity, even though it was ranked sec-moderate by :dveditz). If there was an exploit chain involving this, that would (of course) change.

Severity: -- → S4
Priority: -- → P3

Frederik Braun [:freddy] Assignee
Updated • 1 year ago

Keywords: sec-want

Frederik Braun [:freddy] Assignee
Comment 7 • 1 year ago

Attached file ***Bug 1915257 - refactor webchannel to use actor's principal r=nalexander*** — *Details*

Frederik Braun [:freddy] Assignee
Comment 8 • 1 year ago

I am sharing the proposed patch from ~~comment 4~~ for review. The patch assumes that the parent should "just" use the principal from the actor rather than the event. My try push will help confirming (or rejecting) this theory.

Phabricator Automation
Updated • 1 year ago

Assignee: nobody → fbraun
Status: NEW → ASSIGNED

Julien Wajsberg [:julienw]
Comment 9 • 1 year ago

(In reply to Frederik Braun [:freddy] from ~~comment #8~~)

> I am sharing the proposed patch from ~~comment 4~~ for review. The patch assumes that the parent should "just" use the principal from the actor rather than the event. My try push will help confirming (or rejecting) this theory.

Just a quick note that I believe that the profiler use of the WebChannel isn't tested, it would need manual testing.

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

(In reply to Julien Wajsberg [:julienw] from ~~comment #9~~)

> Just a quick note that I believe that the profiler use of the WebChannel isn't tested, it would need manual testing.

There are a few tests, which set the pref `devtools.performance.recording.ui-base-url` to control the site of the profiler.

Phabricator Automation
Updated • 1 year ago

Attachment #9433862 - Attachment description: WIP: Bug 1915257 - refactor webchannel to use actor's principal r=nalexander → Bug 1915257 - refactor webchannel to use actor's principal r=nalexander

Pulsebot
Comment 11 • 1 year ago

Pushed by fbraun@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/a821eb312fcd
refactor webchannel to use actor's principal r=nalexander,nika

Frederik Braun [:freddy] Assignee
Comment 12 • 1 year ago

(In reply to Julien Wajsberg [:julienw] from ~~comment #9~~)

> Just a quick note that I believe that the profiler use of the WebChannel isn't tested, it would need manual testing.

My bad.. I just landed this due to phabricator comments rather than checking back here. Can you help me identify functionality and how it should be tested in a list of steps to repeat?

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 13 • 1 year ago

https://hg.mozilla.org/mozilla-central/rev/a821eb312fcd

Group: firefox-core-security → core-security-release
Status: ASSIGNED → RESOLVED
Closed: 1 year ago
status-firefox134: --- → fixed
Resolution: --- → FIXED
Target Milestone: --- → 134 Branch

Donal Meehan [:dmeehan]
Updated • 1 year ago

status-firefox132: --- → wontfix
status-firefox133: --- → affected
status-firefox-esr115: --- → wontfix

status-firefox-esr128: --- → affected
tracking-firefox133: --- → +
tracking-firefox134: --- → +
tracking-firefox-esr128: --- → 133+

BugBot [:suhaib / :marco/ :calixte]
Comment 14 • 1 year ago

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

- If yes, please nominate the patch for beta approval.
- If no, please set `status-firefox133` to `wontfix`.

For more information, please visit BugBot documentation.

Flags: needinfo?(fbraun)

Frederik Braun [:freddy] Assignee
Comment 15 • 1 year ago

With the testing situation unclear, I'd rather let this bake for the whole nightly+beta cycle before this hits release.

status-firefox133: affected → wontfix
Flags: ~~needinfo?(fbraun)~~

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

tracking-firefox133: + → ---
tracking-firefox-esr128: 133+ → 134+

Frederik Braun [:freddy] Assignee
Comment 16 • 1 year ago

Who can help me make a decision for upcoming ESR?
Security: This is hardening and we haven't seen it in attacks. Someone looking at the patch for release might use this in attacks. We can't tell.
Stability: We have no indication that this might break something. But we also have no tests.

Mark Hammond [:markh] [:mhammond]
Comment 17 • 1 year ago

I'm not sure if this helps, but setting up a Firefox Account uses webchannels extensively. We've also recently been doing work touching some of the webchannel messages sent and received between desktop

and fxa to support oauth logins, so have been observing this closely and have had dedicated QA testing the new login flows.

Thus, I believe the patch as landed has had recent and testing, and signing in to the browser might offer a reasonable vehicle for checking things are working OK with ESR should the patch land there.

Andrei Vaida [:avaida]
Updated • 1 year ago

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

Frederik Braun [:freddy] Assignee
Comment 18 • 1 year ago

Comment on attachment 9433862 [details]
~~Bug 1915257~~ - refactor webchannel to use actor's principal r=nalexander

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**: Somewhat simple security fix
- **User impact if declined**: Missing alignment with release
- **Fix Landed on Version**: 134
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: The team thinks this is not risky and I agree: There are not a lot of tests, but this isn't changing behavior for the intended code path. Just an extra check that code behaves as we believe it should.

Attachment #9433862 - Flags: approval-mozilla-esr128?

Frederik Braun [:freddy] Assignee
Comment 19 • 1 year ago

The files haven't been touched in a while on ESR, I think the existing patch might apply.

Ryan VanderMeulen [:RyanVM]
Comment 20 • 1 year ago

Comment on attachment 9433862 [details]
~~Bug 1915257~~ - refactor webchannel to use actor's principal r=nalexander

Approved for 128.6esr.

Attachment #9433862 - Flags: approval-mozilla-esr128? → approval-mozilla-esr128+

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

status-firefox-esr128: affected → fixed

Pulsebot
Comment 21 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-esr128/rev/949ad31cb057

Serban Stanca [:SerbanS]
Comment 22 • 1 year ago • Edited

Backed out for causing multiple failures.

- Backout link
- Push with failures - lint failures
- Failure Log
- Failure line: TEST-UNEXPECTED-ERROR | /builds/worker/checkouts/gecko/toolkit/actors/WebChannelChild.sys.mjs:60:26 | 'principal' is not defined. (no-undef)

- Push with failures - mochitests failures
- Failure Log
- Failure line: TEST-UNEXPECTED-FAIL | toolkit/modules/tests/browser/browser_web_channel.js | Test timed out -

---

- Push with failures - mochitests failures
- Failure Log
- Failure line: TEST-UNEXPECTED-FAIL | browser/base/content/test/general/browser_remoteTroubleshoot.js | Test timed out -

Flags: needinfo?(fbraun)

Ryan VanderMeulen [:RyanVM]
Comment 23 • 1 year ago

Does this need rebasing around ~~bug 1275612~~ maybe?

status-firefox-esr128: fixed → affected

Andrew McCreight [:mccr8] Reporter
Comment 24 • 1 year ago

We could uplift ~~bug 1275612~~ if that helps. That just deleted some code that hadn't been doing anything for 2 years. Technically it is a bit of a hardening measure. The only other related fix was ~~bug 1916451~~ for Thunderbird, but that looks like it is just deleting setting a pref behind NIGHTLY_BUILD so surely that doesn't matter.

Frederik Braun [:freddy] Assignee
Updated • 1 year ago

Flags: ~~needinfo?(fbraun)~~

Pulsebot
Comment 25 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-esr128/rev/8a78d2663079

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

status-firefox-esr128: affected → fixed

Frederik Braun [:freddy] Assignee
Updated • 1 year ago

Whiteboard: [adv-main134+][adv-ESR128.6+]

Frederik Braun [:freddy] Assignee
Comment 26 • 1 year ago

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

Frederik Braun [:freddy] Assignee
Updated • 1 year ago

Alias: CVE-2025-0237

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 ↑