Closed Bug 1895342 (CVE-2025-0245) Opened 1 year ago Closed 1 year ago

Firefox Focus security bug: "Use fingerprint to unlock app" bypass

Categories

Product: Focus
Component: General
Platform: Unspecified Android

Type: defect
Priority: P3 Severity: S3

Tracking

Status: RESOLVED FIXED
Milestone: 134 Branch

Tracking Flags:

	Tracking	Status
firefox132	---	wontfix
firefox133	---	wontfix
firefox134	---	fixed

People (Reporter: bugzilla.mozilla.org, Assigned: mcarare)

References

Details (Keywords: csectype-disclosure, reporter-external, sec-moderate, Whiteboard: [fixed by 1930512][client-bounty-form][adv-main134+])

Attachments

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

Show Obsolete

Bottom ↓ Tags Timeline

bugzilla.mozilla.org Reporter
Description • 1 year ago

In Firefox Focus there is a setting that says "Use fingerprint to unlock app". When enabled, the user must first authenticate. The app should be locked if the user does not authenticate.

The bug is that this authentication step can be circumvented allowing fully access to the app (including browser history by pressing the "page back" button, and including the ability to switch to other open tabs).

Steps to reproduce:

- Make sure that Firefox Focus has the "Use fingerprint to unlock app" setting turned on
- Use the app and then put it to the background (home button) or kill it completely (swipe up in task manager). When the app is started, user should authenticate first
- Long-press the desktop and add the search widget
- Quickly press the search widget, the home button and then the Firefox Focus icon
- If done quickly enough, Firefox Focus will open without having to authenticate

I tried to attach a movie showing the bug, but it was too big. I put it online here: https://jurr.org/20240506_Firefox_Focus_unlock_bug/ (Both files are the same movie - pick one.)

0:00 - 0:14: the "Use fingerprint to unlock app" is set
0:15 - 0:45: a little browsing (regular usage)
0:45 - 0:52: shows that the app should be unlocked after putting it to the background
0:52 - 1:01: Add search widget
1:01 - 1:04: Tried to reproduce, but misclicked - sorry!
1:04 - 1:16: Reproduce bug, open app without authentication. Also shows access to "page back", so full access

Note that it does not matter if the app is only put into the background or completely killed ("swiped up in the task manager").

Confirmed on:

- Firefox Focus 125.3.0 (latest) on Android 13 (security update 05-04-2024)
- Firefox Focus 125.3.0 (latest) on Android 9
- Firefox Focus 125.3.0 (latest) on Android 11 (emulator - this is how the movie was recorded)

I'd be very happy to assist in any way I can. Please let me know how.

Flags: sec-bounty?

Andrew McCreight [:mccr8]
Updated • 1 year ago

Group: firefox-core-security → mobile-core-security
Component: Security → General
Product: Firefox → Focus

Daniel Veditz [:dveditz]
Comment 1 • 1 year ago

I couldn't reproduce myself, but sec-moderate if the Focus team can.

Keywords: csectype-disclosure, sec-moderate

bugzilla.mozilla.org Reporter
Comment 2 • 1 year ago

Is there anything I can do to assist?

Flags: needinfo?(dveditz)

Chris Peterson [:cpeterson]
Comment 3 • 1 year ago

Thanks for sharing this bug. Can you also reproduce this bug in (non-Focus) Firefox?

Severity: -- → S3
OS: Unspecified → Android
Priority: -- → P3

bugzilla.mozilla.org Reporter
Comment 4 • 1 year ago

Firefox Focus has the "Use fingerprint to unlock app" setting. This feature request that the user authenticates before the app can be used. The security bug is that this feature can be bypassed, making it completely irrelevant.

Does (non-Focus) Firefox have such a setting? I couldn't find it. Could you tell me where it is?

Flags: needinfo?(cpeterson)

Chris Peterson [:cpeterson]
Comment 5 • 1 year ago

> Does (non-Focus) Firefox have such a setting? I couldn't find it. Could you tell me where it is?

You're correct. I see that Firefox doesn't have such a setting. Sorry!

Flags: ~~needinfo?(cpeterson)~~

David Lawrence [:dkl]
Updated • 1 year ago

Keywords: reporter-external

bugzilla.mozilla.org Reporter
Comment 6 • 1 year ago

It's been well over a month now. I was wondering how much time Mozilla would need until I can make this public?
Again, is there anything I can do to assist? I'd like to help where possible to get this fixed.

bugzilla.mozilla.org Reporter
Comment 7 • 1 year ago

Two months passed now. 😕 Is there something I can do to speed this up?

Flags: needinfo?(dkl)
Flags: needinfo?(cpeterson)
Flags: needinfo?(continuation)

Andrew McCreight [:mccr8]
Updated • 1 year ago

Flags: ~~needinfo?(dkl)~~
Flags: ~~needinfo?(continuation)~~

bugzilla.mozilla.org Reporter
Comment 8 • 1 year ago

Andrew, I think :cpeterson is on the normal Firefox mobile team? This bug is only related to Firefox Focus...

Flags: needinfo?(continuation)

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

I'll see if I can find out who works on fixing Focus security bugs.

Flags: ~~needinfo?(continuation)~~

Daniel Veditz [:dveditz]
Comment 10 • 1 year ago

Timing was tricky, but I was finally able to reproduce this on a real phone.

If you're "too slow" and get the fingerprint lock when you open Focus after the search widget then it seems that after the unlock I get a blank Focus screen (like the search page... ok) and I can't go back to the page I was on before. Hitting the back button closes(?) Focus and returns me to the home page. I'm sure that's unrelated, but a) it's frustrating in general, and b) for purposes of trying to reproduce this bug it means you have to do the "browsing around" step again so you have somewhere for the back button to go.

Flags: ~~needinfo?(dveditz)~~

Daniel Veditz [:dveditz]
Comment 11 • 1 year ago

(In reply to bugzilla.mozilla.org from ~~comment #8~~)

> Andrew, I think :cpeterson is on the normal Firefox mobile team? This bug is only related to Firefox Focus...

We don't have a "Focus team". Focus is built on top of the same GeckoView and android components that Fenix is and is handled by the same team.

bugzilla.mozilla.org Reporter
Comment 12 • 1 year ago

Hi Daniel,

Great that you were able to reproduce! Just to be sure we are on the same page: when I wrote "Also shows access to page back", I meant to illustrate that you have full access to Firefox Focus. Pressing the back button in itself is not part of the steps to reproduce.

Imagine a user that browses a random page, and then close Firefox Focus. This bug would get the attacker that same page, including browsing history. The attack is 100% circumventing the fingerprint unlock screen.

You write that one can be too slow. It might help to add the Firefox Focus launcher to the quick launch section at the bottom. I have it there myself (of course!)

Nice to see this bug report getting some traction; I hope Mozilla can get it fixed. Again: if there's anything I can do to help, please say so 😀

Chris Peterson [:cpeterson]
Updated • 1 year ago

Status: UNCONFIRMED → NEW
Ever confirmed: true
Flags: ~~needinfo?(cpeterson)~~

Mihai Adrian Carare [:mcarare] Assignee
Updated • 1 year ago

Assignee: nobody → mcarare

Mihai Adrian Carare [:mcarare] Assignee
Comment 13 • 1 year ago

This was fixed in 134 cycle.

Status: NEW → RESOLVED
Closed: 1 year ago
status-firefox132: --- → wontfix
status-firefox133: --- → wontfix
status-firefox134: --- → fixed
Resolution: --- → FIXED

Ryan VanderMeulen [:RyanVM]
Comment 14 • 1 year ago

Please add the bug # that fixed this to the "Depends on" field.

Group: mobile-core-security → core-security-release
Flags: needinfo?(mcarare)
Target Milestone: --- → 134 Branch

Mihai Adrian Carare [:mcarare] Assignee
Updated • 1 year ago

Depends on: ~~1930512~~
Flags: ~~needinfo?(mcarare)~~

Daniel Veditz [:dveditz]
Updated • 1 year ago

Flags: sec-bounty? → sec-bounty+
Whiteboard: [reporter-external] [client-bounty-form] [verif?] → [fixed by 1930512][client-bounty-form]

Andrei Vaida [:avaida]
Updated • 1 year ago

QA Whiteboard: [post-critsmash-triage]

Frederik Braun [:freddy]
Updated • 1 year ago

Whiteboard: [fixed by 1930512][client-bounty-form] → [fixed by 1930512][client-bounty-form][adv-main134+]

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

Attached file ~~**advisory.txt**~~ *(obsolete) — Details*

bugzilla.mozilla.org Reporter
Comment 16 • 1 year ago

Hi Frederik,

For the advisory, could you please use my full name? "Jurrie Overgoor" Thanks!

Jurrie

Flags: needinfo?(fbraun)

Frederik Braun [:freddy]
Comment 17 • 1 year ago

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

Fixed.

Attachment #9445551 - Attachment is obsolete: true
Flags: ~~needinfo?(fbraun)~~

Frederik Braun [:freddy]
Updated • 1 year ago

Alias: CVE-2025-0245

Andrew McCreight [:mccr8]
Updated • 1 year ago

See Also: → ~~CVE-2025-1941~~

Daniel Veditz [:dveditz]
Updated • 10 months ago

Group: ~~core-security-release~~

Daniel Veditz [:dveditz]
Updated • 9 months ago

See Also: → ~~1976300~~

You need to log in before you can comment on or make changes to this bug.

Top ↑