Closed Bug 1929584 (CVE-2025-0244) Opened 1 year ago Closed 1 year ago

Android Firefox address bar spoofing through invalid protocols

Categories

Product: Firefox for Android
Component: Browser Engine

Type: defect

Priority: *Not set* Severity: S2

Tracking

Status: RESOLVED FIXED
Milestone: 134 Branch

Tracking Flags:

	Tracking	Status
firefox133	---	wontfix
firefox134	+	fixed

People (Reporter: Puf, Unassigned)

References

Details (Keywords: csectype-spoof, reporter-external, sec-high, Whiteboard: [client-bounty-form][adv-main134+])

Attachments

PufIndex.html Details
1 year ago **Umar Farooq [:Puf]**
1.01 KB, text/html

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

Show Obsolete

Bottom ↓ Tags Timeline

Umar Farooq [:Puf] Reporter
Description • 1 year ago

*Attached file **PufIndex.html** (obsolete) — Details*

In Android Firefox there is a possibility to spoof using `google.com://` and `apple.com://`. When a user clicks on link, it will replace the address bar to `Google.com://` `apple.com://` and changes the entire screen with attacker-controlled content.

the spoofed URL address appear to be very similar to the original attackers this type of altered URLs to trick users into thinking they are on a legitimate website which allows an attacker to spoof the entire

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 analytics. Rest assured, we value your privacy. You will be able to change your Cookie Settings later.
Accept All Cookies
Reject All Non-Essential Cookies

screen with attacker-controlled content.

`Steps to Reproduce:`

1. Open PufIndex.html
2. Click on Open Google Login link🔗

`Result:` Successfully Spoofed URL address to `Google.com://Login`

I have attached video Link 🌐🔗🔒 reproducing the attack. ✅

OS Info 📱:
Firefox Version: [134.0a1]
Operating System: [Android 14 📱]

Thank you

Flags: sec-bounty?

Umar Farooq [:Puf] Reporter
Comment 1 • 1 year ago

(https://youtube.com/shorts/mB4lwIkJofw) = attached Unlisted video Link 🌐🔗🔒 reproducing the attack. ✅

Emma Zühlcke [:emz]
Updated • 1 year ago

Group: firefox-core-security → mobile-core-security
Component: Security → Browser Engine
Product: Firefox → Fenix

Andrew McCreight [:mccr8]
Updated • 1 year ago

Summary: Android Firefox address bar Spoofing → Android Firefox address bar spoofing through invalid protocols

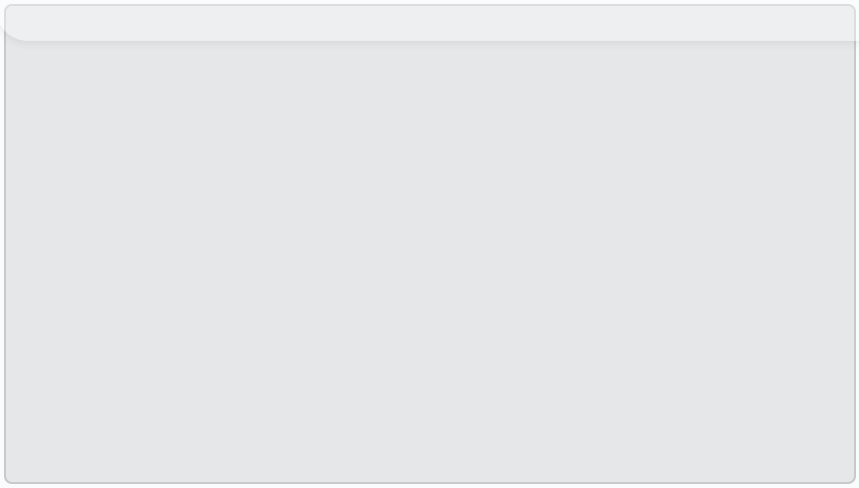
Umar Farooq [:Puf] Reporter
Comment 2 • 1 year ago

Just Adding a Colon `:` to any domain name it works 🌐 `Google.com:` 🌐 `apple.com:`

Umar Farooq [:Puf] Reporter
Comment 3 • 1 year ago

*Attached file **PufIndex.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.



Attachment #9435878 - Attachment is obsolete: true

Umar Farooq [:Puf] Reporter
Comment 4 • 1 year ago

For your information, This Vulnerability effect only on Latest `Firefox Nightly Version: [134.0a1] (Build #20160541750)`

Daniel Veditz [:dveditz]
Comment 5 • 1 year ago

This sounds very similar to the bugs where you could spoof with a broken port: we were displaying the chosen URL first before we loaded it and it never loaded. In that case the server never responded (or eventually timed out). In this case we've gone out to ask the OS if there's support for that protocol and failed, but not clearing the URL bar or reverting to the original page.

On desktop we print the error to the console and simply don't navigate. I have no idea if the error here is the front-end doing the wrong thing or if that error never even makes it out of geckoview to the front-end.

Presumably you could make the lock icon look right if the attack was hosted on an https site (have not tried the attachment yet).

Keywords: csectype-spoof
See Also: → CVE-2025-0246

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.

Daniel Veditz [:dveditz]
Comment 6 • 1 year ago

Not only does it show a lock, if you click the lock it says my connection is secure to "google.com:". How are we populating that dialog? Are we just parsing the URL and figuring that if we could load it that's what it must be? We should be getting that data from the SecurityInfo on the load, and clearly that's not making it out to the front-end

Status: UNCONFIRMED → NEW

Ever confirmed: true
Keywords: sec-high

BugBot [:suhaib / :marco/ :calixte]
Comment 7 • 1 year ago

The severity field is not set for this bug.
:boek, could you have a look please?

For more information, please visit BugBot documentation.

Flags: needinfo?(jboek)

Umar Farooq [:Puf] Reporter
Comment 8 • 1 year ago

looks like this vulnerability is fixed! in Due to latest update in Firefox Nightly 134.0a1

Please kindly Verify and Change Status to fixed

Comment hidden (duplicate)

Andrew McCreight [:mccr8]
Updated • 1 year ago

See Also: → 1932749

Comment hidden (duplicate)

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

Can confirm this is fixed: I could reproduce the bug in 133.0b9 but not in 134.0b1 after I updated (and couldn't reproduce in a 134 nightly). I didn't see any "fixed in 134" Fenix bugs that could account for it.

status-firefox133: --- → affected
status-firefox134: --- → fixed
tracking-firefox134: --- → +
Flags: needinfo?(dveditz)

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.

Daniel Veditz [:dveditz]
Comment 12 • 1 year ago

Bug 1921426 fixed a core Gecko bug with external protocol handlers, but that would only change the behavior for things loaded by a web extension. That can't be the thing that fixed it.

There are also a whole lot of "[toolbar redesign]" bugs that were fixed but those don't look like the fix either. 1) the new design isn't enabled in 134 where this appears fixed, and 2) most of the changes were to the appearance and functionality of buttons and things in the toolbar but not really the functioning of how we update the URL-containing box.

I guess we'll have to do nightly build bisection to narrow this down
https://archive.mozilla.org/pub/fenix/nightly/2024/11/

Group: mobile-core-security → core-security-release
Severity: -- → S2
Flags: ~~needinfo?(jboek)~~

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

Status: NEW → RESOLVED
Closed: 1 year ago
status-firefox133: affected → wontfix
Resolution: --- → FIXED
Target Milestone: --- → 134 Branch

Daniel Veditz [:dveditz]
Comment 13 • 1 year ago

Polly: do you know of what changes might have fixed this? Was it toolbar redesign work? It doesn't seem to be have been fixed as an intentional security fix in some related bug, at least as far as I can see.

Please pass the request on to a better person on the Android team if you weren't part of that work.

Flags: needinfo?(polly)

Umar Farooq [:Puf] Reporter
Comment 14 • 1 year ago

Looks like it is fixed in external protocol section

Click email

external protocol execution is not working in hyperlinks

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.

Daniel Veditz [:dveditz]
Updated • 1 year ago

Duplicate of this bug: 1923749

Polly [:polly]
Comment 16 • 1 year ago

i am not aware of anything that has changed in this area from the android side, and can't see anything obvious from looking at the code.
Maybe [:zmckenney] knows of something that has changed in the toolbar that might have fixed this?

Flags: needinfo?(polly) → needinfo?(zmckenney)

Zac McKenney [:zmckenney]
Comment 17 • 1 year ago

I'm not aware of any work for the redesign that would have affected this and I went back through all of the tickets since October related to the project and didn't see any that could be relevant. I can't be sure this is a Gecko/GeckoView issue but it seems to me like it would be.

Flags: ~~needinfo?(zmckenney)~~

Frederik Braun [:freddy]
Updated • 1 year ago

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

Frederik Braun [:freddy]
Comment 18 • 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-2025-0244

Daniel Veditz [:dveditz]
Updated • 1 year ago

Flags: sec-bounty? → sec-bounty+

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.