Closed Bug 1912709 (CVE-2025-0246) Opened 1 year ago Closed 1 year ago

Android Firefox Nightly Address bar Spoof with SSL Lock via navigation to non-existent protocol

Categories

Product: Firefox for Android
Component: Toolbar
Platform: Unspecified Android

Type: defect
Priority: P3 Severity: S3

Tracking

Status: RESOLVED FIXED

Tracking Flags:

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

People (Reporter: proof131072, Unassigned)

References

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

Attachments

Screen_Recording_20240812_151614_Firefox Nightly.mp4 Details
1 year ago **James Lee**
7.99 MB, video/mp4

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

I'm pretty sure there is better character than "n" to make this spoof better, but you get the idea of how this could be abused for spoofing attack.

PoC demo: https://pwning.geniuscoolcat.com/nttps.php

Flags: sec-bounty?

Andrew McCreight [:mccr8]
Updated • 1 year ago

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

Andrew McCreight [:mccr8]
Updated • 1 year ago

Keywords: csectype-spoof

Andrew McCreight [:mccr8]
Updated • 1 year ago

Keywords: sec-low

James Lee Reporter
Comment 1 • 1 year ago

I believe this is sec-moderate like https://bugzilla.mozilla.org/show_bug.cgi?id=1681103 since it's a spoof with SSL Lock based on Copy/Paste and this one acrually works with popped-up bookmark navigation too.

Chris Peterson [:cpeterson]
Updated • 1 year ago

Severity: -- → S3
Component: General → Toolbar

Daniel Veditz [:dveditz]
Comment 2 • 1 year ago

This appears to be fixed in 134 (beta) but we don't know what fixed it. There were some general toolbar redesign work but I don't know if that touched the address parsing part

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

Daniel Veditz [:dveditz]
Updated • 1 year ago

Group: mobile-core-security → core-security-release

Frederik Braun [:freddy]
Updated • 1 year ago

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

Frederik Braun [:freddy]
Comment 3 • 1 year ago

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

```
Address bar spoofing using an invalid protocol scheme on F
James Lee

When using an invalid protocol scheme, an attacker could s
```

Frederik Braun [:freddy]
Comment 5 • 1 year ago

The browser will treat ssh:// and foobar:// both as invalid. Happy to change that to "unhandled" if you feel strongly.

James Lee Reporter
Comment 6 • 1 year ago

Thank you for the reply and suggestion Frederik, the intention of above reply wasn't for suggesting advisory context change btw (I do agree that both "invalid" and "unhandled" would be appropriate for the description). I just wanted to add info for the context of this issue here that other existing protocols like above could've also been abused for this issue.

👍 1

Frederik Braun [:freddy]
Updated • 1 year ago

Alias: CVE-2025-0246

Simon Friedberger [:simonf]
Updated • 1 year ago

Flags: sec-bounty? → sec-bounty+

Daniel Veditz [:dveditz]
Updated • 10 months ago

Group: ~~core-security-release~~

James Lee Reporter
Comment 7 • 10 months ago