Copy Summary | View

Closed Bug 1651636 (CVE-2020-15665) Opened 3 years ago Closed 3 years ago

Clicking "stay on page" (ie cancelling) in beforeunload dialogs should cause us to reset the URL bar

Categories

Product: Firefox
Component: Tabbed Browser
Type: defect
Priority: Not set Severity: --

Tracking

Status: RESOLVED FIXED
Milestone: Firefox 80
Tracking Flags: firefox80 Tracking --- Status fixed

People (Reporter: Gijs, Assigned: Gijs)

References (Blocks 1 open bug)

Details (Keywords: csectype-spoof, sec-moderate, Whiteboard: [adv-main80+])

Attachments

Bug 1651636 - reset the address bar when beforeunload prompts close, r?mak! — Details | Review
3 years ago :Gijs (he/him)
47 bytes, text/x-phabricator-request

advisory.txt — Details
2 years ago Tom Ritter [:tjr]
344 bytes, text/plain

Bottom ↓ | Tags | Timeline

:Gijs (he/him) Assignee
Description • 3 years ago

The fact that we don't do this is part of a chain of not-quite-right-things used by https://twitter.com/lbherrera_/status/1280617786088329220 and ~~bug 1333599~~. AIUI fixing this will break the spoof. There's an old patch to address this in ~~bug 1333599~~, I think.

Daniel Veditz [:dveditz]
Updated • 3 years ago

Keywords: csectype-spoof, sec-moderate

Daniel Veditz [:dveditz]
Updated • 3 years ago

Blocks: 1481994

Daniel Veditz [:dveditz]
Comment 1 • 3 years ago

... and a different old patch in bug 1481994

Daniel Veditz [:dveditz]
Updated • 3 years ago

Group: ~~firefox-core-security~~

:Gijs (he/him) Assignee
Comment 3 • 3 years ago

*Attached file **Bug 1651636 - reset the address bar when beforeunload prompts close, r?mak!** — Details*

Phabricator Automation
Updated • 3 years ago

Assignee: nobody → gijskruitbosch+bugs
Status: NEW → ASSIGNED

Pulsebot
Comment 4 • 3 years ago

Pushed by gijskruitbosch@gmail.com:
https://hg.mozilla.org/integration/autoland/rev/88fef29ec070
reset the address bar when beforeunload prompts close, r=mak

Bogdan Tara[:bogdan_tara | bogdant]
Comment 5 • 3 years ago • Edited

Backed out changeset 88fef29ec070 (~~bug 1651636~~) for browser_clearSiteData.js failures

Push with failures: https://treeherder.mozilla.org/#/jobs?repo=autoland&group_state=expanded&selectedTaskRun=YKNizO0HSIGID84rCp9ZDQ.0&searchStr=mochitest-browser-chrome&fromchange=9b5c17afe643590abedc963cb8f8bcd794734dcd&tochange=e1eb9b5914f30e4327ad0f46f03c2808c0ccf2ad

Backout link: https://hg.mozilla.org/integration/autoland/rev/e1eb9b5914f30e4327ad0f46f03c2808c0ccf2ad

Failure log: https://treeherder.mozilla.org/logviewer.html#/jobs?job_id=309883299&repo=autoland&lineNumber=12058

```
...
[task 2020-07-15T18:56:06.164Z] 18:56:06     INFO - Entering test bound
[task 2020-07-15T18:56:06.164Z] 18:56:06     INFO - Buffered messages logged at 18:56:02
[task 2020-07-15T18:56:06.164Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.165Z] 18:56:06     INFO - Buffered messages logged at 18:56:04
[task 2020-07-15T18:56:06.165Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.165Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
```

```
[task 2020-07-15T18:56:06.165Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.166Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.166Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.166Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.167Z] 18:56:06     INFO - found chrome://browser/skin/preferences/preference
[task 2020-07-15T18:56:06.167Z] 18:56:06     INFO - found chrome://global/skin/in-content/common.css
[task 2020-07-15T18:56:06.167Z] 18:56:06     INFO - found chrome://browser/skin/preferences/dialog.css
[task 2020-07-15T18:56:06.167Z] 18:56:06     INFO - TEST-PASS | browser/components/preferences/tests/s
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - Buffered messages logged at 18:56:05
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - Console message: OpenGL compositor Initialized Suc
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - Version: 2.1 INTEL-12.9.22
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - Vendor: Intel Inc.
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - Renderer: Intel Iris OpenGL Engine
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - FBO Texture Target: TEXTURE_2D
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - Buffered messages finished
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - TEST-UNEXPECTED-FAIL | browser/components/preferen
[task 2020-07-15T18:56:06.173Z] 18:56:06     INFO - fireDialogEvent@resource://gre/modules/SharedPromp
```

Flags: needinfo?(gijskruitbosch+bugs)

:Gijs (he/him) Assignee
Updated • 3 years ago

Flags: ~~needinfo?(gijskruitbosch+bugs)~~

Pulsebot
Comment 6 • 3 years ago

Pushed by gijskruitbosch@gmail.com:
https://hg.mozilla.org/integration/autoland/rev/8079eea73df3
reset the address bar when beforeunload prompts close, r=mak

Bogdan Tara[:bogdan_tara | bogdant]
Comment 7 • 3 years ago

bugherder

https://hg.mozilla.org/mozilla-central/rev/8079eea73df3

Status: ASSIGNED → RESOLVED
Closed: 3 years ago
status-firefox80: affected → fixed
Resolution: --- → FIXED
Target Milestone: --- → Firefox 80

Tom Ritter [:tjr]
Updated • 2 years ago

Whiteboard: [adv-main80+]

Tom Ritter [:tjr]
Comment 8 • 2 years ago

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

Tom Ritter [:tjr]
Updated • 2 years ago

Alias: CVE-2020-15665

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

Top ↑