Copy Summary ▾ View ▾

Closed Bug 1713259 (CVE-2021-29975) Opened 2 years ago Closed 2 years ago

Show form reportValidity validationMessage on any website

▾ **Categories**

Product: Toolkit ▾
Component: XUL Widgets ▾

Type: defect
Priority: *Not set* Severity: --

▾ **Tracking**

Status: RESOLVED FIXED
Milestone: 91 Branch

Tracking Flags:

	Tracking	Status
firefox-esr78	---	unaffected
firefox88	---	wontfix
firefox89	---	wontfix
firefox90	---	fixed
firefox91	---	fixed

▸ **People** (Reporter: sourc7, Assigned: enndeakin)

▸ **References** (Regression)

▸ **Details** (Keywords: csectype-spoof, regression, sec-moderate, Whiteboard: [reporter-external] [client-bounty-form] [verif?][adv-main90+])

▾ **Attachments**

spoof.bundle.html
2 years ago **Irvan Kurniawan (:sourc7)**
1.69 KB, text/html
Details

Firefox - Spoof reportValidity validationMessage on Twitter.mp4
2 years ago **Irvan Kurniawan (:sourc7)**
719.07 KB, video/mp4
Details

spoof.bundle.cleanmessage.html
2 years ago **Irvan Kurniawan (:sourc7)**
1.68 KB, text/html
Details

Firefox - Spoof reportValidity validationMessage on Twitter with Clean Message.mp4
2 years ago **Irvan Kurniawan (:sourc7)**
707.71 KB, video/mp4
Details

Bug 1713259, hide form validation popup when switching pages, r=gijs
2 years ago **Neil Deakin**
48 bytes, text/x-phabricator-request
jcristau : **approval-mozilla-beta+** Details | Review

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

Bottom ↓ Tags ▾ Timeline ▾

Irvan Kurniawan (:sourc7) Reporter
Description • 2 years ago
−

Attached file ***spoof.bundle.html*** *— Details*

After set `reportValidity()` as `canvas.toBlob` callback and set `contenteditable` to `true` , the reportValidity validationMessage will persist even the tab was closed. As the validationMessage is persist on the screen, after the tab was closed the validationMessage still show to previous active tab.

In this report I demonstrate I able to spoof validationMessage on Twitter then overlap the Twitter button intent (which press enter also works) to retweet/like the tweet.

As the validationMessage is showed on secure domain, user will likely trust the message is from the website, and the validationMessage will overlap Twitter button intent message so user won't notice that press enter will retweet/like the tweet.

Mozregression show it is regression of Bug 1684792, open form validation popup anchored at screen coordinate as datetime picker and select do so that it is positioned correctly in out of process iframes

Affected version:

- Firefox Nightly 90.0a1 (2021-05-27) (64-bit)
- Firefox Release 88.0.1 (64-bit)

Unaffected version:

- Firefox 78.10.1esr (64-bit)

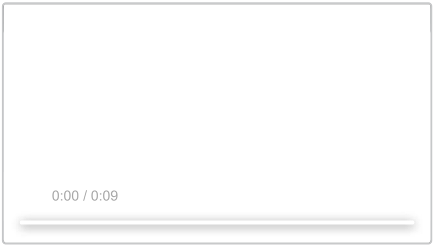
Steps to Reproduce:

1. Visit attached spoof.bundle.html
2. Click "Spoof validationMessage" button
3. Validation message appear on Twitter website
4. If you're logged in then press Enter to like the tweet

Flags: sec-bounty?

Irvan Kurniawan (:sourc7) Reporter
Comment 1 • 2 years ago

Attached video ***Firefox - Spoof reportValidity validationMessage on Twitter.mp4*** *— Details*



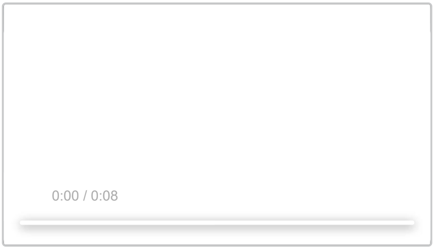
Irvan Kurniawan (:sourc7) Reporter
Comment 2 • 2 years ago

Attached file ***spoof.bundle.cleanmessage.html*** *— Details*

Hereby I attached the testcase with invisible unicode symbol on custom validationMessage.

Irvan Kurniawan (:sourc7) Reporter
Comment 3 • 2 years ago

Attached video ***Firefox - Spoof reportValidity validationMessage on Twitter with Clean Message.mp4*** *— Details*



Daniel Veditz [:dveditz]
Comment 4 • 2 years ago

I can confirm this. When I try it the validation panel doesn't cover the twitter "like" confirmation as in the video, but it's still present and that's the heart of the problem. I assume in a real attack the differences could be researched and accounted for (OS? site custom zoom level? fonts?), and even if not, the panel contents will be assumed to come from the visibly showing site and could be used for various other spoofs.

Type: task → defect
status-firefox88: --- → wontfix
status-firefox89: --- → affected
status-firefox90: --- → affected
status-firefox-esr78: --- → unaffected
Component: Security → XUL Widgets
Flags: needinfo?(enndeakin)
Keywords: csectype-spoof
Product: Firefox → Toolkit
Regressed by: ~~1684792~~

BMO Automation
Updated • 2 years ago

Has Regression Range: --- → yes
Keywords: regression

Neil Deakin Assignee
Comment 5 • 2 years ago

Attached file ***Bug 1713259, hide form validation popup when switching pages, r=gijs*** *— Details*

Phabricator Automation
Updated • 2 years ago

Assignee: nobody → enndeakin
Status: NEW → ASSIGNED

Irvan Kurniawan (:sourc7) Reporter
Updated • 2 years ago

Summary: Show reportValidity validationMessage on any website → Show form reportValidity validationMessage on any website

Neil Deakin Assignee
Comment 6 • 2 years ago

Gijs mentioned that the security severity needs to be set to land this.

Flags: needinfo?(enndeakin) → needinfo?(dveditz)

Daniel Veditz [:dveditz]
Updated • 2 years ago

Flags: ~~needinfo?(dveditz)~~
Keywords: sec-moderate

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 7 • 2 years ago

hide form validation popup when switching pages, r=Gijs
https://hg.mozilla.org/integration/autoland/rev/7324f82612ca091548dc32f2b2756a22c0a3d6b5
https://hg.mozilla.org/mozilla-central/rev/7324f82612ca

Group: firefox-core-security → core-security-release
Status: ASSIGNED → RESOLVED
Closed: 2 years ago
status-firefox91: --- → fixed
Resolution: --- → FIXED
Target Milestone: --- → 91 Branch

:Gijs (he/him)
Comment 8 • 2 years ago

Does this want uplift to 90? And have you put the test up in a separate bug somewhere so we can land that after we ship the fix? :-)

Flags: needinfo?(enndeakin)

Ryan VanderMeulen [:RyanVM]
Updated • 2 years ago

status-firefox89: affected → wontfix

Neil Deakin Assignee
Comment 9 • 2 years ago

Comment on attachment 9224284 [details]
~~Bug 1713259~~, hide form validation popup when switching pages, r=gijs

Beta/Release Uplift Approval Request

- **User impact if declined**: A page can popup up an invalid form with a custom message and then redirect to another page, possibly tricking the user into thinking they are on another page.
- **Is this code covered by automated tests?**: Yes
- **Has the fix been verified in Nightly?**: Yes
- **Needs manual test from QE?**: No
- **If yes, steps to reproduce**: Automated test will be in another bug.
- **List of other uplifts needed**: None
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**:
- **String changes made/needed**: None

Flags: ~~needinfo?(enndeakin)~~
Attachment #9224284 - Flags: approval-mozilla-beta?

Julien Cristau [:jcristau]
Comment 10 • 2 years ago

Comment on attachment 9224284 [details]
~~Bug 1713259~~, hide form validation popup when switching pages, r=gijs

approved for 90.0b5

Attachment #9224284 - Flags: approval-mozilla-beta? → approval-mozilla-beta+

Julien Cristau [:jcristau]
Comment 11 • 2 years ago
uplift

https://hg.mozilla.org/releases/mozilla-beta/rev/2a5a6bc641a4

status-firefox90: affected → fixed
Flags: in-testsuite?

Daniel Veditz [:dveditz]
Comment 12 • 2 years ago

Severity is on the low end of moderate, but the combination is clever and we are awarding a bounty for it. In this particular example it's not entirely convincing due to the ugliness of the prompt, but it might just confuse people enough to work.

"on top" elements strike again :-(

Flags: sec-bounty? → sec-bounty+

Cornel Ionce [:noni] [Hubs QA]

Updated • 2 years ago

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

Tom Ritter [:tjr]
Updated • 2 years ago

Whiteboard: [reporter-external] [client-bounty-form] [verif?] → [reporter-external] [client-bounty-form] [verif?][adv-main90+]

Tom Ritter [:tjr]
Comment 13 • 2 years ago

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

Tom Ritter [:tjr]
Updated • 2 years ago

Alias: CVE-2021-29975

Daniel Veditz [:dveditz]
Updated • 1 year ago

Group: ~~core-security-release~~

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

Top ↑