










☆ Starred by 3 users

Owner: mustaq@chromium.org

CC: gov...@chromium.org
adetaylor@chromium.org
 sjclement@google.com
 penaganti.ganga@chromium.org
japhet@chromium.org
 nzolghadr@chromium.org
domenic@chromium.org
 emilyschechter@chromium.org
bl...@google.com
pbomm...@chromium.org
 vstar@google.com
mustaq@chromium.org
 creis@chromium.org
 ppetrenk@google.com
 aemiller@google.com
mmanchala@chromium.org
alex...@chromium.org
yaoxia@chromium.org
hexed@google.com
 vanditha.podduturi@chromium.org
solomonkinard@chromium.org
tjudkins@chromium.org

Status: Verified (Closed)

Components: Platform>Extensions
UI>Browser>Navigation
Blink>SecurityFeature>IFrameSandbox

Modified: Jun 4, 2020

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Windows, Chrome, Mac

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
.allpublic

Issue 1035315: iframe sandbox allow_top_navigation_by_user_activation can be bypassed with certain extensions

Reported by alexandre.leborgne.83@gmail.com on Wed, Dec 18, 2019, 3:50 AM EST

🔗 Code

Chrome Version : 78.0.3904.108 (Build official) (64 bits) (cohort: Stable)

URLs (if applicable) : http://w3c-test.org/html/semantics/embedded-content/the-iframe-element/iframe_sandbox_allow_top_navigation_by_user_activation-manual.html

What steps will reproduce the problem?

- (1) Open the link
- (2)
- (3)

What is the expected result?

You should not be redirected and the page should show at the bottom:
The sandboxed iframe should post a message saying the top navigation was blocked when no user gesture.

You should see the error in console :

iframe-that-performs-top-navigation.html:7 Unsafe JavaScript attempt to initiate navigation for frame with URL 'http://w3c-test.org/html/semantics/embedded-content/the-iframe-element/iframe_sandbox_allow_top_navigation_by_user_activation-manual.html' from frame with URL 'http://w3c-test.org/html/semantics/embedded-content/the-iframe-element/support/iframe-that-performs-top-navigation.html'. The frame attempting navigation of the top-level window is sandboxed with the 'allow-top-navigation-by-user-activation' flag, but has no user activation (aka gesture). See <https://www.chromestatus.com/feature/5629582019395684>.

What happens instead?

You are redirect to <http://w3c-test.org/html/semantics/embedded-content/the-iframe-element/support/navigation-changed-iframe.html>

The page contains :
"PASSED: Navigation succeeded."

If you click on the link and you quickly stop loading the page before the redirection then you do F5, the page works correctly and the redirection is done only when clicking on the button in the iframe

Comment 1 by vanditha.podduturi@chromium.org on Wed, Dec 18, 2019, 12:23 PM EST

Labels: Needs-Triage-M78

Comment 2 by penaganti.ganga@chromium.org on Thu, Dec 19, 2019, 8:31 AM EST

Cc: penaganti.ganga@chromium.org
Labels: Triaged-ET Needs-Feedback

Tested the issue on reported chrome version#78.0.3904.108 using Mac 10.14.6 by the following steps:
Steps:

1. Navigated to the given link - 'http://w3c-test.org/html/semantics/embedded-content/the-iframe-element/iframe_sandbox_allow_top_navigation_by_user_activation-manual.html'
2. Observed error in console 'Unsafe JavaScript attempt to'
3. On clicking the 'Navigate the top page' button, it is redirecting to this link - '<http://w3c-test.org/html/semantics/embedded-content/the-iframe-element/support/navigation-changed-iframe.html>'

Attached screencast for reference.

@Reporter: Could you please review the attached screencast and confirm if this is the issue you are pointing to.

Thanks...

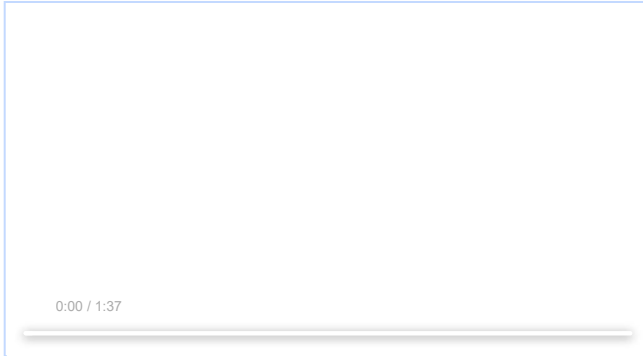
[Deleted] 1035315.mp4

Comment 3 by alexandre.leborgne.83@gmail.com on Thu, Dec 19, 2019, 12:54 PM EST

Your screencast does not show the bug.

Here is a video that shows that the problem seems random. You can see that sometimes I am redirected (when it shouldn't be) and sometimes not.

1035315 - ifram sandbox llow_top_navigation_by_user_activation does not work as expected - chromium - An open-source project to help move the web forward. - Monorail - Google Chrome 2019-12-19 18-44-11~1.mp4
3.0 MB [View](#) [Download](#)



Comment 4 by sheriffbot@chromium.org on Thu, Dec 19, 2019, 12:59 PM EST

Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

Comment 5 by tkent@chromium.org on Sun, Dec 22, 2019, 8:49 PM EST

Components: -Blink Blink>SecurityFeature

Comment 6 by mkwst@chromium.org on Tue, Dec 24, 2019, 4:46 AM EST

Owner: domenic@chromium.org

Cc: -domenic@chromium.org

Assigning to domenic@ for triage, as the others listed on the chromestatus entry aren't actually on the project anymore.

Comment 7 by mkwst@chromium.org on Tue, Dec 24, 2019, 4:47 AM EST

Cc: jahpet@chromium.org

Components: -Blink>SecurityFeature Blink>SecurityFeature>IFrameSandbox UI>Browser>Navigation

Also +jahpet, FYI.

Comment 8 by domenic@chromium.org on Mon, Jan 6, 2020, 4:36 PM EST

Cc: yaoxia@chromium.org

Yao, I know you've been working on sandboxed downloads. This feature is related and seems likely to be in the same area; is your team an appropriate owner for it, who could help wit htthe triaging?

Comment 9 by yaoxia@chromium.org on Mon, Jan 6, 2020, 6:54 PM EST

Cc: mustaq@chromium.org

I'm able to reproduce on current stable build (M79) though it seems rare/random, but I couldn't reproduce it on the ToT build.

@mustaq: Do you know if anything got fixed recently around user activation that may have fixed the bug like this?

Comment 10 by mmanchala@chromium.org on Wed, Jan 22, 2020, 5:23 AM EST

Cc: mmanchala@chromium.org

Gentle ping:

mustaq@ : Could you please provide update on bug

Thanks..!!

Comment 11 by mustaq@chromium.org on Wed, Jan 22, 2020, 10:32 AM EST

Summary: iframe sandbox allow_top_navigation_by_user_activation does not work as expected (was: ifram sandbox llow_top_navigation_by_user_activation does not work as expected)

alexandre.leborgne.83@gmail.com: I couldn't reproduce the bug on 79.0.3945.130. Please give us more details about your setup:

- Which OS are you using?
- Can you reproduce after disabling all extensions (through chrome://extensions)?
- Does it repro for you in latest Chrome beta (M80)?

Comment 12 by alexandre.leborgne.83@gmail.com on Wed, Jan 22, 2020, 2:16 PM EST

I tried to activate / deactivate my extensions and it turns out that this bug is due to this extension (<https://chrome.google.com/webstore/detail/adblock-plus-free-ad-bloc/cfhldojbkjnhkbpkdaibdcddilifdbb>) which causes this security vulnerability.

I'm using Windows 10.0.18362

I can't try on the M80 version

Comment 13 by vanditha.podduturi@chromium.org on Wed, Jan 29, 2020, 4:02 AM EST

Cc: vanditha.podduturi@chromium.org

Gentle ping:

mustaq@ : As per the [comment#12](#), could you please provide further inputs.

Thanks..!!

[Comment 14](#) by mustaq@chromium.org on Wed, Jan 29, 2020, 11:01 AM EST

Status: Available (was: Unconfirmed)

Owner: ----

Cc: domenic@chromium.org

Labels: Pri-2 Type-Bug-Security

Components: Platform>Extensions

Thanks alexandre.leborgne.83@gmail.com for spotting the root cause.

We were able to repro the bug on both Windows and Mac! And also through a different ad-blocker extension:

<https://chrome.google.com/webstore/detail/adblock-%E2%80%94best-ad-blocker/gighmmpiobkifepjocnamgkbbigldom>

Given the popularity of these extension, I am making this bug P2.

[Comment 15](#) by mustaq@chromium.org on Wed, Jan 29, 2020, 11:01 AM EST

Cc: nzolghadr@chromium.org

[Comment 16](#) by mustaq@chromium.org on Wed, Jan 29, 2020, 11:04 AM EST

Summary: iframe sandbox allow_top_navigation_by_user_activation can be bypassed with certain extensions (was: iframe sandbox allow_top_navigation_by_user_activation does not work as expected)

[Comment 17](#) by mustaq@chromium.org on Wed, Jan 29, 2020, 11:21 AM EST

Labels: OS-Linux OS-Mac OS-Windows

[Comment 18](#) by mmoroz@chromium.org on Wed, Jan 29, 2020, 11:39 AM EST

Labels: Security_Impact-Stable Security_Severity-Medium M-81 OS-Chrome

[Comment 19](#) by sheriffbot@chromium.org on Wed, Jan 29, 2020, 11:59 AM EST

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

[Comment 20](#) by mmoroz@google.com on Mon, Feb 3, 2020, 7:19 PM EST

Status: Assigned (was: Available)

Owner: mustaq@chromium.org

All security bugs must have an owner. mustaq@, let me please assign this to you for the time being. Please re-assign if needed.

[Comment 21](#) by mustaq@chromium.org on Wed, Feb 5, 2020, 12:17 PM EST

Cc: alex...@chromium.org creis@chromium.org

Found a consistent repro, see below. The core problem is that switching tabs by clicking on the tab-strip allows the bypass to happen within the first 5 seconds.

IMHO, browser UI clicks allowing the bypass seems bad. The mentioned ad-blockers seem very popular, and there may be other extensions that repro this.

[Repro steps]

1. Install any of the ad-blocker extensions mentioned above.
2. Go to this test wrapper page:
`data:text/html,test link`
3. Right click on the link, then choose "open in a new tab".
4. Click on the tab-strip to switch away then come back to the test link tab. Within 5 seconds right click on the link to open it in a new tab.
5. Repeat Step 4 but wait for more than 5 seconds.

[Outcome]

Tabs opened through Step 3 and Step 5 correctly prevents navigation, but the tab opened through Step 4 navigates away without user interaction.

[Comment 22](#) by mustaq@chromium.org on Wed, Feb 5, 2020, 3:08 PM EST

Good news is that none of the tab content is activated. On receiving tabs.onActivated event, the background script gets activated here, which seems reasonable.

Still not sure why the content-initiated navigation is affected by the background activation state.

[1] <https://cs.chromium.org/chromium/src/extensions/renderer/dispatcher.cc?rcl=d90d3c6341c9c65834e39fcd149b2dbbcd9ddc&l=1058>

[Comment 23](#) Deleted

[Comment 24](#) by mustaq@chromium.org on Wed, Feb 5, 2020, 5:15 PM EST

My last comment was partially wrong...all new tabs gets activated for those ad blockers even though tab-click doesn't activate them directly:

- Click on tab-strip sends tabs.onActivated event to the background script only and activates it.

- Upon navigation, the ad blockers send messages to navigated tab through this code [1], which activates the page.

[1] https://cs.chromium.org/chromium/src/extensions/renderer/native_renderer_messaging_service.cc?rcl=ba08c24e87fe57098cfe562967dfb328cda9547e&l=319

[Comment 25](#) by sheriffbot on Thu, Feb 20, 2020, 10:52 AM EST

mustaq: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

[Comment 26](#) by mustaq@chromium.org on Thu, Feb 20, 2020, 11:06 AM EST

Blockedon: 957633

This is blocked on a reasonable and non-breaking fix for extension messaging user activation. See blocker Issue 957633.

Comment 27 by mustaq@chromium.org on Mon, Feb 24, 2020, 2:40 PM EST

Cc: hexed@google.com

Comment 28 by [bugdroid](#) on Wed, Feb 26, 2020, 4:30 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+6f9f33b66f3b94918efcdd41768a40b7c5e3df13>

commit [6f9f33b66f3b94918efcdd41768a40b7c5e3df13](#)

Author: Mustaq Ahmed <mustaq@google.com>

Date: Wed Feb 26 21:29:00 2020

Extension: remove USER_GESTURE_ENABLED state from tab-change events.

A past fix for activation propagation from an extension button to extension script seems to have added additional user activation propagation path from tab-strip to all installed extensions: <https://chromiumcodereview.appspot.com/10821120/>

This crack caused every tab-switching to activate /all/ installed extensions, which seems bad. Because of this, we encountered a security issue with unintended top frame navigation from an iframe. (Luckily only tab switching was affected, not tab clicking.)

A user interaction with the tab-strip is different from an interaction with extension buttons. Tab-strip interactions are similar to those on any browser-provided UI element like top menu; they don't at all indicate the user's intention to interact with any extension or website. Therefore, like clicks on top-menu and unlike clicks on extension buttons, tab-switching should suppress activating any background script thus prevent access to use user-activation gated APIs like popup, fullscreen, navigation, etc.

Bug: 957633, [4955345](#)

Change-Id: [I8d56e02a3a2966521b7bbc4f4efad67e1acc371](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2072654>

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Commit-Queue: Mustaq Ahmed <mustaq@chromium.org>

Cr-Commit-Position: refs/heads/master@{#744802}

[modify] https://crrev.com/6f9f33b66f3b94918efcdd41768a40b7c5e3df13/chrome/browser/extensions/api/tabs/tabs_event_router.cc

[modify] https://crrev.com/6f9f33b66f3b94918efcdd41768a40b7c5e3df13/chrome/browser/extensions/api/tabs/tabs_event_router.h

Comment 29 by mustaq@google.com on Wed, Feb 26, 2020, 5:02 PM EST

Status: Fixed (was: Assigned)

Note: to verify the fix, please follow the consistent repro steps in [#c21](#).

Comment 30 by [sheriffbot](#) on Thu, Feb 27, 2020, 2:05 PM EST

Labels: Restrict-View-SecurityNotify

Comment 31 by natashapabrai@google.com on Mon, Mar 2, 2020, 12:54 PM EST

Labels: reward-topanel

Comment 32 by [sheriffbot](#) on Mon, Mar 2, 2020, 2:28 PM EST

Labels: Merge-Request-81

Requesting merge to beta M81 because latest trunk commit (744802) appears to be after beta branch point (737173).

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

Comment 33 by [sheriffbot](#) on Mon, Mar 2, 2020, 2:31 PM EST

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: M81's targeted beta branch promotion date has already passed, so this requires manual review. Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on master/Tot?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: benmason@(Android), bindusuvama@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

Comment 34 by mustaq@chromium.org on Mon, Mar 2, 2020, 3:28 PM EST

Status: Verified (was: Fixed)

Here are most of the answers:

1. This is a very simple change.
2. CL to merge: <https://chromium-review.googlesource.com/c/chromium/src/+2072654>
3. I just verified the fix in latest Win Canary (82.0.4075.0), with each of the ad blockers above.
4. "See below."
5. Not a new feature.
6. N/A.

Q4 (M81 vs M82) is a tricky question. If malicious subframes (possibly in ads) discover this, they could cause lots of user annoyances and could cause false clicks in ads. The old behavior has been there for many years, and we don't know if it has been abused in the wild or if it has got attention already. So I am slightly biased towards M81.

mmoroz@chromium.org, alexmos@chromium.org: what's your opinion from security perspective?

Comment 35 by pbommana@google.com on Tue, Mar 3, 2020, 2:27 PM EST

Cc: adetaylor@chromium.org pbomm...@chromium.org gov...@chromium.org

+adetaylor@ (Security TPM) for M81 merge review

[Comment 36](#) by adetaylor@chromium.org on Tue, Mar 3, 2020, 3:15 PM EST

Labels: -Merge-Review-81 Merge-Rejected-81

I think I'm going to decline this merge to M81. Thanks for the answers though mustaq@. My rationale is that this is a Medium severity bug, and we only merge mediums back if it's trivially low-risk in every respect. Although the patch is trivial, this does (deliberately) change behavior which faces web developers and/or extension developers. Whilst it's probably very unlikely that any legitimate developers are relying on this functionality, we can't entirely rule it out. So I think we should organically release this in M82 so they have maximum possible time to react.

[Comment 37](#) by mustaq@chromium.org on Tue, Mar 3, 2020, 3:17 PM EST

Sounds good, given that the bug has been there for years already.

[Comment 38](#) by natashapabrai@google.com on Thu, Mar 5, 2020, 12:06 PM EST

Labels: -reward-topanel reward-unpaid reward-1000

*** Boilerplate reminders! ***

Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.

[Comment 39](#) by natashapabrai@google.com on Thu, Mar 5, 2020, 12:09 PM EST

Congrats! The Panel decided to award \$1,000 for this report!

[Comment 40](#) by natashapabrai@google.com on Thu, Mar 5, 2020, 12:15 PM EST

Labels: -reward-unpaid reward-inprocess

[Comment 41](#) by alexandre.leborgne.83@gmail.com on Fri, Mar 6, 2020, 3:30 PM EST

Hello, Thank you for the attention you have given to my report.

I wish to claim the reward. I am a resident of France. What information is necessary for you and by what means should I communicate it to you?

[Comment 42](#) by adetaylor@chromium.org on Fri, Mar 6, 2020, 3:34 PM EST

Hi alexandre.leborgne.83, thanks again for the report! You don't need to do anything - someone from our finance team will get in touch with you.

How would you like to be credited in the Chrome release notes? (At present this isn't planned to be released until M82 so it will be a while before it appears.)

[Comment 43](#) by alexandre.leborgne.83@gmail.com on Fri, Mar 6, 2020, 3:43 PM EST

No idea ... what is normally done and where does it appear? In the commit message?

You can use :

Alexandre Le Borgne <alexandre.leborgne.83@gmail.com>

[Comment 44](#) by bi...@google.com on Fri, Mar 6, 2020, 3:57 PM EST

Cc: ppetrenk@google.com vstar@google.com sjclement@google.com

[Comment 45](#) by adetaylor@chromium.org on Fri, Mar 6, 2020, 7:46 PM EST

Re #c43, thanks, I'll just use your name. It appears on <https://chromereleases.googleblog.com/>.

[Comment 46](#) by mustaq@chromium.org on Mon, Mar 9, 2020, 10:34 AM EDT

Labels: -M-81 M-82

[Comment 47](#) by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT

Labels: Release-0-M83

[Comment 48](#) by adetaylor@chromium.org on Mon, May 18, 2020, 11:58 AM EDT

Labels: CVE-2020-6476 CVE_description-missing

[Comment 49](#) by adetaylor@chromium.org on Wed, May 20, 2020, 11:43 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

[Comment 50](#) by mustaq@chromium.org on Thu, May 21, 2020, 11:29 AM EDT

Blocking: 957633

[Comment 51](#) by mustaq@chromium.org on Thu, May 21, 2020, 11:29 AM EDT

Blockedon: -957633

[Comment 52](#) by sheriffbot on Thu, Jun 4, 2020, 2:59 PM EDT

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot