☆ Starred by 4 users

Owner:	jkarlin@chromium.org
CC:	a...@chromium.org jkarlin@chromium.org sjclement@google.com csharrison@chromium.org janag...@google.com aaronherrmann@google.com vstar@google.com hexed@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>PopupBlocker
Modified:	Sep 21, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Target-88
Target-87
Target-89
Target-90
Merge-Rejected-90
merge-merged-4240
M-91
LTR-Merged-86
LTS-Security-86
Target-91
external_security_report
merge-merged-4430
merge-merged-90

Issue 1145553: bypass blocked autoredirects from cross-origin iframes

Reported by el...@confiant.com on Wed, Nov 4, 2020, 8:55 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36

Steps to reproduce the problem:
Hi Team,

Current versions of desktop and mobile web browsers including Chrome, Safari, Edge, Opera, and Brave will block automatic redirects that are not activated by user interaction from cross-origin iframes.

Consider the following payload that will always get blocked when served in a cross-origin iframe:

```
<script>
    top.window.location = "https://google.com";
</script>
```

There exists a bug that bypasses this built-in mitigation and it's currently being leveraged as part of a malvertising chain to bypass the browser's redirect protection in order to drive traffic to malware.

The following payload is being used:

```
<script type="text/javascript">
  var x = '<html><body><script type="text/javascript"> window.top.location = "https://google.com";' + '</scr' + 'ipt></body></html>';
  var bs64 = btoa(x);
  document.write('<iframe sandbox="allow-top-navigation allow-scripts" src="data:text/html;base64,' + bs64 + '"></iframe>')
</script>
```

We have observed through testing that the sandbox parameters in the injected frame are key in in the bypass here.

The following browsers have been tested and proven to be vulnerable:

- Chrome Desktop, Android, and iOS
- Edge Desktop
- Safari Desktop, iOS
- Edge Desktop
- Opera Desktop, Android
- Brave Desktop, Android

A note on impact:

This bug is being actively abused by a malvertising group that we at Confiant have dubbed Yosec, serving fake flash drive-by downloads and tech support scams. They have been able to successfully run their malicious ads on dozens of high profile websites, including those among the Comscore top 100. On November 3rd, their activity was running at such high volumes that we have observed up to 0.5% of all United States ad impressions at certain times.

We hope that you will prioritize a fix for this soon considering how disruptive and damaging malvertising campaigns like this can be.

Best,
Eliya Stein of Confiant

What is the expected behavior?
Automatic redirects from cross-origin iframes should be blocked by the browser.

What went wrong?
This is being bypassed with the payload provided above.

Did this work before? N/A

Chrome version: 86.0.4240.111 Channel: n/a
OS Version: OS X 10.15.7
Flash Version:

Comment 1 by sheriffbot on Wed, Nov 4, 2020, 8:59 AM EST   Project Member
Labels: reward-potential

Comment 2 by awhalley@google.com on Wed, Nov 4, 2020, 12:43 PM EST   Project Member
Cc: hexed@google.com hexed@google.com vstar@google.com aaronherrmann@google.com sjclement@google.com

Comment 3 by kenrb@chromium.org on Thu, Nov 5, 2020, 10:39 AM EST   Project Member
Labels: OS-Android OS-Chrome OS-Linux OS-Windows
Components: Blink>SecurityFeature>IFrameSandbox

Thanks for the report.

To clarify, the JS code you are providing is from loaded in an ad iframe, correct? Is that iframe also sandboxed with the same flags?

Comment 4 by el...@confiant.com on Thu, Nov 5, 2020, 10:48 AM EST

Hi,

Yes, the payload loads from within an ad iframe, typically a DFP Safe Frame, or any other cross-origin iframe.

The redirect will occur automatically if the iframe does not have additional sandboxing properties.

However, redirects like this would typically be blocked by the browser otherwise if not for the funky payload.

Best,
Eliya

Comment 5 by hexed@google.com on Thu, Nov 5, 2020, 11:00 AM EST   Project Member
Status: Untriaged (was: Unconfirmed)
Labels: Security_Impact-Stable Security_Severity-Medium
Components: UI>Browser>PopupBlocker

Thank you for your report. This is more of a popup blocker bypass that an iframe sandbox one.

Were able to reproduce with this:

~~~
publisher.origin: `<iframe src='advertiser.origin'></iframe>` // no sandbox, but is cross-origin
advertiser.origin (malicious) : ```
<iframe sandbox="allow-top-navigation allow-scripts" /* allow-top-navigation takes precedence over cross-origin */
  srcdoc="<script> window.top.location = 'http://example.com' </script>">
</iframe>
~~~

Comment 6 by el...@confiant.com on Thu, Nov 5, 2020, 11:05 AM EST

Thanks for the feedback @hexed - I appreciate the additional context!

Comment 7 by sheriffbot on Thu, Nov 5, 2020, 1:03 PM EST   Project Member
Labels: M-87 Target-87

Setting milestone and target because of Security_Impact=Stable and medium severity.

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

Comment 8 by sheriffbot on Thu, Nov 5, 2020, 1:39 PM EST   Project Member
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 9 by kenrb@chromium.org on Fri, Nov 6, 2020, 7:35 PM EST   Project Member
Components: -Blink>SecurityFeature>IFrameSandbox

Comment 10 by kenrb@chromium.org on Fri, Nov 6, 2020, 9:27 PM EST   Project Member
Status: Assigned (was: Untriaged)
Owner: a...@chromium.org

avi@ are you able to have a look at this? Or else would you know a better owner?

Comment 11 by a...@chromium.org on Fri, Nov 6, 2020, 11:09 PM EST   Project Member
Owner: csharrison@chromium.org
Cc: a...@chromium.org

I'm super busy with various Mac launches. Charlie, can you poke at this?

Comment 12 by sheriffbot on Wed, Nov 18, 2020, 12:21 PM EST   Project Member

csharrison: 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 13 by sheriffbot on Wed, Dec 2, 2020, 12:21 PM EST   Project Member csharrison: Uh oh! This issue still open and hasn't been updated in the last 28 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 14 by csharrison@chromium.org on Thu, Dec 3, 2020, 3:39 PM EST Project Member

Cc: jkarlin@chromium.org

Comment 15 by jkarlin@chromium.org on Thu, Dec 3, 2020, 4:56 PM EST Project Member

The allow-top-navigation attribute is the embedder specifically allowing the sandboxed iframe to navigate the top frame without a gesture. This is working as intended. allow-top-navigation-by-user-activation should be used if the embedder doesn't want the frame to be able to navigate the top frame.

Comment 16 by jkarlin@chromium.org on Thu, Dec 3, 2020, 4:57 PM EST Project Member

Posted to soon, meant to say "if the embedder doesn't want the frame to be able to navigate the top frame without a user gesture".

Comment 17 by el...@confiant.com on Thu, Dec 3, 2020, 5:12 PM EST

@jkarlin - Thanks for your feedback, but I'm not sure that this is actually working as intended. If the top frame embeds a cross-origin iframe with a basic redirect along the lines of top.location = xxxx, then the browser prevents the redirection.

The payload supplied in the example above bypasses that block.

The example that we provided is not being run in the top frame, but rather this code is being run inside a cross-origin iframe:

```
<script type="text/javascript">
  var x = '<html><body><script type="text/javascript"> window.top.location = "https://google.com";' + '</scr' + 'ipt></body></html>';
  var bs64 = btoa(x);
  document.write('<iframe sandbox="allow-top-navigation allow-scripts" src="data:text/html;base64,' + bs64 + '"></iframe>')
</script>
```

This is currently being abused in malvertising campaigns to launch forced redirections from ad slots where the redirect would normally be blocked.

If this behavior is intentional, then I don't believe that cross-origin frames would block basic redirections in the first place as they consistently do these days.

Comment 18 by jkarlin@chromium.org on Thu, Dec 3, 2020, 6:03 PM EST Project Member

Sorry, I didn't realize that the sandboxed iframe was itself placed in a cross-origin iframe to the embedder. Yes, that does seem like a bug.

Comment 19 by jkarlin@chromium.org on Fri, Dec 4, 2020, 12:21 PM EST Project Member

Owner: jkarlin@chromium.org

I'll take a look.

Comment 20 by jkarlin@chromium.org on Fri, Dec 4, 2020, 12:21 PM EST Project Member

Cc: csharrison@chromium.org

Comment 21 by el...@confiant.com on Tue, Dec 22, 2020, 2:54 PM EST

Hey Team,

I just wanted to share with you all that Apple has acknowledged the issue as it pertains to safari and will be looking to fix it after the new year.

Not sure if this helps you in any way, but thought I'd offer an update.

Best,
Eliya

Comment 22 by sheriffbot on Wed, Jan 20, 2021, 12:22 PM EST Project Member

Labels: -M-87 Target-88 M-88

Comment 23 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 24 by el...@confiant.com on Thu, Jan 21, 2021, 8:50 AM EST

Hi Team - I just got confirmation that Apple will be rolling out the webkit fix in an upcoming patch. Curious if there's a timeline for a fix in Chrome just so that we can prepare a coordinated disclosure that doesn't compromise any impacted vendor.

Thanks,
Eliya

Comment 25 by el...@confiant.com on Mon, Feb 8, 2021, 9:28 AM EST

Hi Team,

Just as an FYI this bug was assigned CVE-2021-1765 for Webkit.

Best,
Eliya

Comment 26 by jkarlin@chromium.org on Wed, Feb 10, 2021, 7:22 PM EST Project Member

Status: Started (was: Assigned)

I've put together a basic fix in http://crrev.com/c/2688360. Will flesh it out tomorrow.

Comment 27 by est...@chromium.org on Wed, Feb 24, 2021, 2:32 PM EST Project Member

jkarlin, are there any updates on https://chromium-review.googlesource.com/c/chromium/src/+/2688360?

Comment 28 by jkarlin@chromium.org on Wed, Feb 24, 2021, 2:36 PM EST Project Member

Bah, I just checked and my response to Daniel wasn't sent. It was sitting as a draft. Sent, will find a solution.

Comment 29 by bugdroid on Mon, Mar 1, 2021, 2:23 PM EST Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/c732f0ddc0573a0926d39b2f20c81591057c2878

commit c732f0ddc0573a0926d39b2f20c81591057c2878
Author: Josh Karlin <jkarlin@chromium.org>
Date: Mon Mar 01 19:19:08 2021

Prevent sandboxed frames escaping user-gesture intervention

What: This CL ensures that sandboxed iframes with "allow-top-navigation" can't
navigate the top frame if their embedder can't.

How: If the source frame is sandboxed and has allow-top-navigation, it
calls CanNavigate() recursive on its ancestors to see if they are
able to navigate the top frame. If not, return false. One can stop
calling recursively once the first non-sandboxed ancestor has been
checked.

Details: CanNavigate() is a LocalFrame method, but ancestor frames
may be remote. So in this CL CanNavigate's contents are extracted into
a static CanNavigateHelper method that works with both Frame*. The
LocalFrame* bits are only necessary on the initial call to CanNavigate,
and not the recursive calls which might be remote.

~~Bug: 1145553~~
Change-Id: I52474431d868f4f515918845784fe30f69c8c918
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688360
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Josh Karlin <jkarlin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#858644}

[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation.html
[modify] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/renderer/core/frame/local_frame.cc
[modify] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/renderer/core/frame/local_frame.h
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/flag-specific/disable-site-isolation-trials/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox-expected.txt
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox.html
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-expected.txt
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/cross-iframe-that-performs-top-navigation-in-nested-sandboxed-frame.html
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox-expected.txt
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/cross-iframe-that-performs-top-navigation-in-sandboxed-frame.html
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/failed-top-navigation.html
[add] https://crrev.com/c732f0ddc0573a0926d39b2f20c81591057c2878/third_party/blink/web_tests/flag-specific/disable-site-isolation-trials/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-expected.txt

Comment 30 by sheriffbot on Wed, Mar 3, 2021, 12:22 PM EST Project Member

Labels: -M-88 Target-89 M-89

Comment 31 by adetaylor@google.com on Wed, Mar 10, 2021, 4:31 PM EST Project Member

jkarlin@ do you consider #c29 a complete fix? If so please mark this as Fixed.

Comment 32 by sheriffbot on Wed, Mar 10, 2021, 8:04 PM EST Project Member

Labels: reward-potential

Comment 33 by zhangtiff@google.com on Wed, Mar 17, 2021, 7:12 PM EDT Project Member

Labels: -reward-potential external_security_bug

Comment 34 by jkarlin@chromium.org on Tue, Apr 6, 2021, 12:32 PM EDT Project Member

Status: Fixed (was: Started)

Whoops, sorry for missing your comment earlier. Yes, this should be fixed now.

Comment 35 by adetaylor@google.com on Tue, Apr 6, 2021, 12:33 PM EDT Project Member

Thanks!

Comment 36 by sheriffbot on Tue, Apr 6, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 37 by el...@confiant.com on Tue, Apr 6, 2021, 1:10 PM EDT

Hi Team,

We have been waiting for the fix to be confirmed before doing a public disclosure, is it safe to do so now?

Thanks,
Eliya

Comment 38 by sheriffbot on Tue, Apr 6, 2021, 1:56 PM EDT Project Member

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 39 by sheriffbot on Tue, Apr 6, 2021, 2:21 PM EDT Project Member

Labels: Merge-Request-90

Requesting merge to beta M90 because latest trunk commit (858644) appears to be after beta branch point (857950).

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

Comment 40 by sheriffbot on Tue, Apr 6, 2021, 2:25 PM EDT Project Member

Labels: -Merge-Request-90 Merge-Review-90 Hotlist-Merge-Review

This bug requires manual review: We are only 6 days from stable.
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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: govind@(Android), bindusuvarna@(iOS), cindyb@(ChromeOS), srinivassista@(Desktop)

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

Comment 41 by adetaylor@google.com on Tue, Apr 6, 2021, 3:09 PM EDT Project Member

Re #c37: Hi Eliya, unfortunately not. The bug will be opened to the public 14 weeks after it's officially marked "Fixed", in order to give time (a) for us to release the fix, which may be M90 next week but might be somewhat later, (b) for our users to absorb that fix (it takes a while for everyone to restart their browsers) and (c) for downstream Chromium browser vendors to absorb the fix. This last reason is the main reason for the long-seeming 14 week delay.

So you'll be able to talk about this publicly 14 weeks after today. We're a bit flexible on that exact date if you have a specific event in mind, but that's the default.

Of course, it's your bug so you're welcome to talk about it whenever you like, but these are the guidelines for it to be VRP-eligible.

Thanks very much for the report!

Comment 42 by el...@confiant.com on Tue, Apr 6, 2021, 3:17 PM EDT

Thanks for the explanation. We will hold off on sharing the details for now.

Comment 43 by jkarlin@chromium.org on Tue, Apr 6, 2021, 3:55 PM EDT Project Member

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

This is an abuse fix rather than pure security, as it allows x-origin frames to navigate the top frame without having first received a user gesture. The code is moderately complex, and has a small chance to break platform behavior. It has been in canary/dev for 3 weeks now, so that increases confidence.

2. Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2688360

3. Has the change landed and been verified on ToT?
Change was landed 3 weeks ago. Verified via tests.

4. Does this change need to be merged into other active release branches (M-1, M+1)?
Just M90

5. Why are these changes required in this milestone after branch?
Because it's a way around our abuse intervention.

6. Is this a new feature?
No.

7. If it is a new feature, is it behind a flag using finch?
No.

Comment 44 by adetaylor@google.com on Tue, Apr 6, 2021, 4:09 PM EDT Project Member

Labels: -Merge-Review-90 Merge-Rejected-90

Discussed with jkarlin@ offline, and we're concerned that there's a slim chance that this could have unexpected compatibility implications. I'm therefore rejecting merge to M90 and this will be released in M91, which will give us and the wider community 6 weeks more to spot any such implications.

Comment 45 by amyressler@google.com on Thu, Apr 22, 2021, 7:56 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 46 by amyressler@chromium.org on Fri, Apr 23, 2021, 6:06 PM EDT Project Member

Hi, Eliya! Congratulations, the VRP Panel has decided to award you $5000 for this report. Nice work and quality report!

Comment 47 by amyressler@chromium.org on Fri, Apr 23, 2021, 6:08 PM EDT Project Member

eliya@ I also meant to mention to please look out for the emails I sent to the VRP researcher community about changes with the payment process! It will temporarily affect payment process starting this week.

Comment 48 by el...@confiant.com on Mon, Apr 26, 2021, 8:55 AM EDT

Thanks Amy! Excited to share this with my team :)

Comment 49 by amyressler@google.com on Mon, Apr 26, 2021, 10:43 AM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 50 by amyressler@chromium.org on Mon, May 24, 2021, 11:28 AM EDT Project Member

Labels: Release-0-M91

Comment 51 by amyressler@google.com on Mon, May 24, 2021, 2:18 PM EDT Project Member

Labels: CVE-2021-30533 CVE_description-missing

Comment 52 by janag...@google.com on Tue, May 25, 2021, 8:43 AM EDT Project Member

Cc: janag...@google.com
Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 53 by sheriffbot on Tue, May 25, 2021, 12:22 PM EDT Project Member

Labels: -M-89 M-90 Target-90

Comment 54 by gianluca@google.com on Wed, May 26, 2021, 11:52 AM EDT Project Member
Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 55 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 56 by asumaneev@google.com on Tue, Jun 8, 2021, 10:54 AM EDT Project Member
Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 57 by sheriffbot on Tue, Jun 8, 2021, 12:22 PM EDT Project Member
Labels: -M-90 M-91 Target-91

Comment 58 by gianluca@google.com on Wed, Jun 9, 2021, 10:47 AM EDT Project Member
Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 59 by Git Watcher on Wed, Jun 9, 2021, 12:47 PM EDT Project Member
Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/8fab4012a41825999014bc83ab253891edeef3c9

commit 8fab4012a41825999014bc83ab253891edeef3c9
Author: Josh Karlin <jkarlin@chromium.org>
Date: Wed Jun 09 16:45:58 2021

[M90-LTS] Prevent sandboxed frames escaping user-gesture intervention

What: This CL ensures that sandboxed iframes with "allow-top-navigation" can't
navigate the top frame if their embedder can't.

How: If the source frame is sandboxed and has allow-top-navigation, it
calls CanNavigate() recursive on its ancestors to see if they are
able to navigate the top frame. If not, return false. One can stop
calling recursively once the first non-sandboxed ancestor has been
checked.

Details: CanNavigate() is a LocalFrame method, but ancestor frames
may be remote. So in this CL CanNavigate's contents are extracted into
a static CanNavigateHelper method that works with both Frame*. The
LocalFrame* bits are only necessary on the initial call to CanNavigate,
and not the recursive calls which might be remote.

(cherry picked from commit c732f0ddc0573a0926d39b2f20c81591057c2878)

~~Bug: 1145553~~
Change-Id: I52474431d868f4f515918845784fe30f69c8c918
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688360
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Josh Karlin <jkarlin@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#858644}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2947088
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Artem Sumaneev <asumaneev@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1507}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/renderer/core/frame/local_frame.cc
[modify] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/renderer/core/frame/local_frame.h
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/flag-specific/disable-site-isolation-trials/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-expected.txt
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/flag-specific/disable-site-isolation-trials/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox-expected.txt
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/cross-iframe-that-performs-top-navigation-in-nested-sandboxed-frame.html
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/cross-iframe-that-performs-top-navigation-in-sandboxed-frame.html
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/failed-top-navigation.html
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-expected.txt
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox-expected.txt
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox.html
[add] https://crrev.com/8fab4012a41825999014bc83ab253891edeef3c9/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation.html

Comment 60 by asumaneev@google.com on Wed, Jun 9, 2021, 1:05 PM EDT Project Member
Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 61 by Git Watcher on Mon, Jun 14, 2021, 3:35 PM EDT Project Member
Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb

commit 6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb
Author: Jana Grill <janagrill@google.com>
Date: Mon Jun 14 19:34:13 2021

[M86-LTS] Prevent sandboxed frames escaping user-gesture intervention

What: This CL ensures that sandboxed iframes with "allow-top-navigation" can't
navigate the top frame if their embedder can't.

How: If the source frame is sandboxed and has allow-top-navigation, it
calls CanNavigate() recursive on its ancestors to see if they are

able to navigate the top frame. If not, return false. One can stop calling recursively once the first non-sandboxed ancestor has been checked.

Details: CanNavigate() is a LocalFrame method, but ancestor frames may be remote. So in this CL CanNavigate's contents are extracted into a static CanNavigateHelper method that works with both Frame*. The LocalFrame* bits are only necessary on the initial call to CanNavigate, and not the recursive calls which might be remote.

M86 merge conflicts and resolution:
* third_party/blink/renderer/core/frame/local_frame.cc
  crrev.com/c/2579744 changes PrintNavigationErrorMessage to report
  "Unsafe attempt" instead of "Unsafe JavaScript attempt". The CL is
  missing from M86 which causes test failures for current CL if
  merged as is. Keep old message with JavaScript and update *.txt
  files to use it.

(cherry picked from commit c732f0ddc0573a0926d39b2f20c81591057c2878)

~~Bug: 1145553~~
Change-Id: I52474431d868f4f515918845784fe30f69c8c918
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688360
Commit-Queue: Josh Karlin <jkarlin@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#858644}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2915720
Commit-Queue: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1671}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/renderer/core/frame/local_frame.cc
[modify] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/renderer/core/frame/local_frame.h
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/flag-specific/disable-site-isolation-trials/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-expected.txt
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/flag-specific/disable-site-isolation-trials/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox-expected.txt
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/cross-iframe-that-performs-top-navigation-in-nested-sandboxed-frame.html
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/cross-iframe-that-performs-top-navigation-in-sandboxed-frame.html
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/resources/failed-top-navigation.html
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-expected.txt
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox-expected.txt
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation-nested-sandbox.html
[add] https://crrev.com/6599d28cc87459bfc3f20f7e4eab9a783ad2bfdb/third_party/blink/web_tests/http/tests/security/frameNavigation/sandbox-DENIED-cross-origin-top-navigation.html

Comment 62 by asumaneev@google.com on Mon, Jun 14, 2021, 3:59 PM EDT Project Member

Labels: -LTS-Merge-Approved-86 LTR-Merged-86

Comment 63 by sheriffbot on Tue, Sep 21, 2021, 1:31 PM EDT Project Member

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