Starred by 3 users

Owner:	ahemery@chromium.org
CC:	creis@chromium.org arthu...@chromium.org nmehta@google.com clamy@chromium.org wfh@chromium.org ajgo@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Sandbox>SiteIsolation UI>Browser>Navigation Blink>SecurityFeature>COOP
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	2
Type:	Bug-Security

reward-2000
Security_Severity-Low
Arch-x86_64
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
FoundIn-99
Security_Impact-Extended
Release-0-M102
CVE-2022-1873

Issue 1305394: Leaking window.length without opener reference.

Reported by ndevtk@protonmail.com on Thu, Mar 10, 2022, 5:59 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36

Steps to reproduce the problem:
1. https://example.com/ run open(); // cross origin page
2. opener.location = 'https://first-party-test.glitch.me/?coop=same-origin'; // Page with COOP
3. let frame = document.createElement('iframe'); f.src = "https://example.org"; document.body.appendChild(f); // Must be cross origin
4. In context of iframe do parent.opener.length to get a new length just create a new cross origin iframe.

You can replace example.com, example.org first-party-test.glitch.me (coop page) with any other origin.

What is the expected behavior?
parent.opener.closed = true (when opener has coop)
It allows leaking the window.length from a coop protected page and after the user has changed the url in the address bar.

What went wrong?
parent.opener.closed = false (when opener has coop)

Did this work before? N/A

Chrome version: 99.0.4844.51 Channel: stable
OS Version: 10.0

Comment 1 by sheriffbot on Thu, Mar 10, 2022, 6:05 PM EST Project Member

Labels: external_security_report

Comment 2 by ndevtk@protonmail.com on Thu, Mar 10, 2022, 10:11 PM EST

By frame I mean f
I noticed sometimes length is not correct if that happens just create a new cross-origin iframe.

Comment 3 by bookholt@google.com on Mon, Mar 14, 2022, 1:25 PM EDT Project Member

Cc: creis@chromium.org
Components: UI>Browser>Navigation

Thanks for the report! Could you please elaborate on the security impact? In other words, what would a malicious website do with this behavior to the detriment of web users?

Comment 4 by creis@chromium.org on Mon, Mar 14, 2022, 1:50 PM EDT Project Member

Owner: arthu...@chromium.org
Labels: OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Lacros

Components: Blink>SecurityFeature>COOP Internals>Sandbox>SiteIsolation

Sounds like this might be a small data leak for COOP? When the opener is navigated to a COOP page, it should go to a new browsing context group (BrowsingInstance), making it inaccessible to the popup. It does look like an injected iframe in the popup can see iframes in the opener (via RemoteFrames / RenderFrameProxies), though, which shouldn't happen. Maybe there's an issue with creating proxies across BrowsingInstances?

This doesn't seem particularly severe unless you can do things with those frames, but it is an information leak that COOP was designed to prevent. Arthur, can you take a look and help triage or find an owner? Thanks!

Comment 5 by arthu...@chromium.org on Mon, Mar 14, 2022, 2:19 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: ahemery@chromium.org
Cc: arthu...@chromium.org
Labels: FoundIn-99 Security_Severity-Low

Thank you for the reproducer! I was skeptical, but this is indeed reproducible.
Here is a video (see attachment)

When you check from the parent "opener" you get null.
However when you check from the child: "parent.opener" you get something not null.
This is not expected.

It looks like when the iframe is same-site with the opener, it is able to "reconstruct" proxies, even if we previously cleared them.

+ahemery@ since you did the implementation, this might be something you would like to take? Happy to help or discuss it.

Comment 6 by sheriffbot on Mon, Mar 14, 2022, 2:27 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 7 by ahemery@chromium.org on Wed, Mar 16, 2022, 12:09 PM EDT Project Member

Having a look! I am able to reproduce and that's indeed very weird...

Comment 8 by Git Watcher on Mon, Mar 28, 2022, 4:37 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e465928a544ccec77e292cd46720f3d1122aa832

commit e465928a544ccec77e292cd46720f3d1122aa832
Author: Arthur Hemery <ahemery@chromium.org>
Date: Mon Mar 28 08:36:15 2022

Fix COOP-based opener removal on FrameTreeNodes.

When a page A opens a page B, B can access A via window.opener. If
either of these pages navigate causing a BrowsingInstance swap, the
links need to be severed. Currently it only works well if B navigates.

If A navigates, we do not find the frames that were opened by it and
remove their openers on the browser side. This is now done in the
RenderFrameHostManager.

We also clarify how this information is carried to the renderer, which

We also clarify how this information is carried to the renderer, which was quite obscure and maybe even involuntary. Explains that the RenderView suppression will trigger an opener clear.

~~BUG=1305394~~

Change-Id: I4bb2a9733c523dac78ffb270877ba07aba6984a4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3532010
Reviewed-by: Arthur Sonzogni <arthursonzogni@chromium.org>
Commit-Queue: Arthur Hemery <ahemery@chromium.org>
Cr-Commit-Position: refs/heads/main@{#985876}

[modify]
https://crrev.com/e465928a544ccec77e292cd46720f3d1122aa832/content/browser/renderer_host/render_frame_host_manager.cc
[modify]
https://crrev.com/e465928a544ccec77e292cd46720f3d1122aa832/content/browser/renderer_host/frame_tree_node.h
[modify]
https://crrev.com/e465928a544ccec77e292cd46720f3d1122aa832/content/browser/renderer_host/frame_tree_node.cc
[modify]
https://crrev.com/e465928a544ccec77e292cd46720f3d1122aa832/content/browser/cross_origin_opener_policy_browsertest.cc

Comment 9 by sheriffbot on Tue, Mar 29, 2022, 2:19 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 10 by ahemery@chromium.org on Mon, Apr 4, 2022, 5:20 AM EDT Project Member

Note for myself: this is fixed but I need to write WPTs to make sure the behavior is implemented by other browsers as well.

Comment 11 by Git Watcher on Mon, Apr 11, 2022, 3:55 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b465304f25945922b9cf68b7e8bf74c056871ecf

commit b465304f25945922b9cf68b7e8bf74c056871ecf
Author: Arthur Hemery <ahemery@chromium.org>
Date: Mon Apr 11 19:53:56 2022

WPT for opener navigations with COOP.

COOP is used to sever relationships with openers, protecting from side-channel attacks. This can happen both when opening popups and when navigating, and that essentially relies on the same mechanism.

When a popup navigates, we do all the opener clearing very nicely and everything ends up in a good state. When the page that opened the popup navigates instead, we do not have as much coverage and some exploits were discovered on Chrome (see associated bug, and fix patch: https://chromium-review.googlesource.com/c/chromium/src/+/3532010)

This patch adds minimal coverage.

Bug: 1305394

~~Bug: 1305394~~
Change-Id: I0d1158acf8ba4521eba272c2a9d6170f60b8bd94
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3578744
Reviewed-by: Arthur Sonzogni <arthursonzogni@chromium.org>
Commit-Queue: Arthur Hemery <ahemery@chromium.org>
Cr-Commit-Position: refs/heads/main@{#991150}

[add] https://crrev.com/b465304f25945922b9cf68b7e8bf74c056871ecf/third_party/blink/web_tests/external/wpt/html/cross-origin-opener-policy/coop-popup-opener-navigates.https.html.headers
[add] https://crrev.com/b465304f25945922b9cf68b7e8bf74c056871ecf/third_party/blink/web_tests/external/wpt/html/cross-origin-opener-policy/coop-popup-opener-navigates.https.html

Comment 12 by ahemery@chromium.org on Tue, Apr 12, 2022, 4:10 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 13 by sheriffbot on Tue, Apr 12, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 14 by sheriffbot on Tue, Apr 12, 2022, 1:40 PM EDT Project Member

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

Comment 15 by amyressler@google.com on Thu, Apr 21, 2022, 8:40 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 16 by ndevtk@protonmail.com on Thu, Apr 21, 2022, 9:33 PM EDT

Thanks :)

Comment 17 by amyressler@chromium.org on Thu, Apr 21, 2022, 10:03 PM EDT Project Member

You're welcome! Thanks for your efforts and reporting this issue to us. :)

Comment 18 by amyressler@google.com on Mon, Apr 25, 2022, 4:22 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 19 by amyressler@chromium.org on Mon, May 23, 2022, 9:58 PM EDT Project Member

Labels: Release-0-M102

Comment 20 by amyressler@google.com on Tue, May 24, 2022, 2:17 PM EDT Project Member

Labels: CVE-2022-1873 CVE_description-missing

Comment 21 by sheriffbot on Wed, Jul 20, 2022, 1:32 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

Comment 22 by amyressler@chromium.org on Thu, Jul 21, 2022, 2:45 PM EDT Project Member

Cc: nmehta@google.com

Comment 23 by amyressler@google.com on Wed, Jul 27, 2022, 5:26 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 24 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing