bugs chromium ▾ New issue Open issues ▾ Search chromium issue ▾ Sign in

☆ Starred by 5 users

Owner:	japhet@chromium.org
CC:	rakina@chromium.org domenic@chromium.org lukasza@chromium.org wfh@chromium.org creis@chromium.org ajgo@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Sandbox>SiteIsolation UI>Browser>Navigation
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Lacros
Pri:	1
Type:	Bug-Security

reward-5000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-94
M-94
FoundIn-93
Security_Impact-Extended
Release-0-M97
CVE-2022-0108

Issue 1248444: Guessing the URL a cross-origin iframe was redirected to by listening to the load event

Reported by herre...@gmail.com on Fri, Sep 10, 2021, 12:06 PM EDT

Code

VULNERABILITY DETAILS
It is possible to try to guess the URL that a cross-origin iframe was redirected to by listening to the load event of the iframe and then redirecting it to the URL you are trying to guess appended by a random hash.

After that, there are two possible outcomes:
1. If you redirect the iframe to the correct URL the iframe was redirected to, no load event will be triggered.
2. If you redirect the iframe to a different URL the iframe was redirected to, the load event will be triggered.

An attacker then would be able to infer the URL of a cross-origin iframe and thus leak sensitive information that shouldn't be available to the attacker.

This likely happens because a navigation to the current URL is treated as a soft reload and it doesn't trigger the load event (unlike a normal navigation).

This issue is similar to bug 1208614 but instead, it leverages and exploits the load event rather than the changes in history.length.

VERSION
Chrome Version: 93.0.4577.63 (Official Build) (64-bit)
Chrome Version: 95.0.4638.0 (Official Build) (64-bit)
Operating System: Windows 10

REPRODUCTION CASE
1. Download both "me.php" and "victimName.php" and host the files in a PHP server (this is needed to simulate the server a victim is accessing).
2. Download "attack.html" (you don't need to host it on a server).
3. In the "attack.html" file you will need to change the domains in the URLs located in the "tryToGuessURL" function calls so that they match the correct domain of your server. By default, the attack is assuming the files can be found on "http://localhost/victimName.php" and "http://localhost/me.php".
4. Open the "attack.html" file and after a few seconds two alert dialogs will show up saying whether you correctly guessed the URL that the iframe was redirected or not.

CREDIT INFORMATION
Reporter credit: Luan Herrera (@lbherrera_)

me.php
224 bytes View Download

victimName.php
66 bytes View Download

attack.html
1.0 KB View Download

Comment 1 by sheriffbot on Fri, Sep 10, 2021, 12:10 PM EDT Project Member

Comment 1 by sheriffbot on Fri, Sep 10, 2021, 12:10 PM EDT Project Member

Labels: external_security_report

Comment 2 by adetaylor@google.com on Fri, Sep 10, 2021, 2:44 PM EDT Project Member

Owner: lukasza@chromium.org
Labels: FoundIn-93 Security_Severity-High
Components: Internals>Sandbox>SiteIsolation

This reproduction case works for me on Ubuntu (Redshell). Packages I needed to install (some of which probably weren't necessary)
sudo apt-get install php7.2-mysql php-db php7.2-mbstring php7.2-curl php7.2-zip php7.2-gd php7.2-intl apache2 php libapache2-mod-php
then put the two files in /var/www/html, chmod a+r and it works just as described. I used ASAN 902206, which is ~M93.

So I think this is a valid cross-origin leak. Cross-origin data leaks are high severity. I think this may well be mitigated down to Medium severity by the need for the attacker to guess specific URIs, but I'll leave the site isolation team to modify the severity if they think so. (Medium would also better match https://bugs.chromium.org/p/chromium/issues/detail?id=1208614#c36).

lukasza@, would you mind taking a look here and trying to route this to the right person?

Comment 3 by adetaylor@google.com on Fri, Sep 10, 2021, 2:45 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Labels: OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1

Comment 4 by sheriffbot on Fri, Sep 10, 2021, 2:46 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 5 by lukasza@chromium.org on Fri, Sep 10, 2021, 3:29 PM EDT Project Member

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

+domenic@ since it seems that this aspect of navigation behavior is web visible and therefore changes here should probably affect specs and/or other browsers

Comment 6 by lukasza@chromium.org on Fri, Sep 10, 2021, 3:31 PM EDT Project Member

Owner: japhet@chromium.org
Cc: lukasza@chromium.org

Let me tentatively assign to japhet@ who has kindly worked on fixing the earlier issue 1208614. I wonder if a similar fix (never treating cross-origin-initiated navigations as same-doc or soft reload) might be possible here.

Comment 7 by creis@chromium.org on Fri, Sep 10, 2021, 3:52 PM EDT Project Member

Labels: -Security_Severity-High Security_Severity-Medium

Comment 2: I think I agree this sounds like Medium severity, based on your note and issue https://bugs.chromium.org/p/chromium/issues/detail?id=1208614#c36. Happy to correct it if it turns out to be worse than that.

Comment 8 by sheriffbot on Sat, Sep 11, 2021, 12:56 PM EDT Project Member

Labels: Target-94 M-94

Setting milestone and target because of medium severity.

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

Comment 9 by sheriffbot on Fri, Sep 24, 2021, 12:21 PM EDT Project Member

japhet: 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 10 by japhet@chromium.org on Wed, Sep 29, 2021, 7:04 PM EDT Project Member

If I'm reading the repro correctly and observing existing behavior, what's happening is that we don't fire onload for cross-origin *same-document* navigations. If the cross-origin initiator provides the exact url of its victim, a soft-reload happens, and because that counts as a cross-document naivgation (i.e., there is a new document object), we fire onload. But when only the fragment changes, we reuse the same document, and we don't fire onload in that case (for either inner window or the iframe element).

I'll see what breaks if we always fire iframe onload for cross-origin-initiated same-document navigations.

Comment 11 by japhet@chromium.org on Thu, Sep 30, 2021, 6:47 PM EDT Project Member

Cc: rakina@chromium.org

Comment 12 by rakina@chromium.org on Thu, Oct 7, 2021, 12:35 AM EDT Project Member

Interesting! I think we should go by "is direct parent cross-origin or not" instead of "is initiator cross origin or not", which is a bit different than the history.length bug (crbug.com/1208614). With the history.length bug, it's possible for any frame to observe history.length, so it makes sense to use initiator. With the iframe load event, I think only the direct parent (the one who actually embeds the iframe) can observe the event, and a same-origin parent might have more assumptions about the timing of the load events of its same-origin child frame (so firing load events in more occasions might break some of those assumptions).

Comment 13 by Git Watcher on Thu, Oct 14, 2021, 4:25 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5f8ddef5a678553c9bb1491cd5710788e6d571b3

commit 5f8ddef5a678553c9bb1491cd5710788e6d571b3
Author: Nate Chapin <japhet@chromium.org>
Date: Thu Oct 14 20:24:32 2021

Fire iframe onload for cross-origin-initiated same-document navigations

A cross-origin initiator can check whether or not onload fired to
guess the url of a target frame. Always firing onload makes it

guess the url of a target frame. Always firing onload makes it appear to be a cross-document navigation, even when it wasn't.

~~Bug: 1248444~~
Change-Id: I79249cb441f61ac6cab65ab9e5dd4a44b291bc4a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3193885
Commit-Queue: Nate Chapin <japhet@chromium.org>
Reviewed-by: Rakina Zata Amni <rakina@chromium.org>
Cr-Commit-Position: refs/heads/main@{#931681}

[modify] https://crrev.com/5f8ddef5a678553c9bb1491cd5710788e6d571b3/third_party/blink/web_tests/http/tests/navigation/same-origin-fragment-navigation-is-sync-expected.txt
[modify] https://crrev.com/5f8ddef5a678553c9bb1491cd5710788e6d571b3/third_party/blink/web_tests/http/tests/navigation/same-origin-fragment-navigation-is-sync.html
[modify] https://crrev.com/5f8ddef5a678553c9bb1491cd5710788e6d571b3/third_party/blink/web_tests/http/tests/navigation/cross-origin-fragment-navigation-is-async-expected.txt
[modify] https://crrev.com/5f8ddef5a678553c9bb1491cd5710788e6d571b3/third_party/blink/web_tests/http/tests/navigation/cross-origin-fragment-navigation-is-async.html
[modify] https://crrev.com/5f8ddef5a678553c9bb1491cd5710788e6d571b3/third_party/blink/renderer/core/loader/document_loader.cc

Comment 14 by sheriffbot on Fri, Oct 15, 2021, 12:21 PM EDT Project Member

japhet: 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 15 by sheriffbot on Tue, Oct 26, 2021, 11:15 AM EDT Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 16 by japhet@chromium.org on Wed, Oct 27, 2021, 1:45 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 17 by sheriffbot on Fri, Oct 29, 2021, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 18 by sheriffbot on Fri, Oct 29, 2021, 1:40 PM EDT Project Member

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

Comment 19 by amyressler@google.com on Wed, Nov 3, 2021, 1:53 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 20 by amyressler@chromium.org on Wed, Nov 3, 2021, 2:22 PM EDT Project Member

Congratulations, Luan! The VRP panel has decided to award you $5000 for this report! Thanks for this report and nice work!

Comment 21 by amyressler@google.com on Thu, Nov 4, 2021, 4:29 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 22 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:29 PM EST Project Member

Labels: Release-0-M97

Comment 23 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0108 CVE_description-missing

Comment 24 by sheriffbot on Wed, Feb 2, 2022, 1:34 PM EST 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 25 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted