Starred by 3 users

Owner:	antoniosartori@chromium.org
CC:	mkwst@chromium.org clamy@chromium.org pmeuleman@chromium.org antoniosartori@chromium.org arthu...@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>SecurityFeature>ContentSecurityPolicy
Modified:	Jun 24, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2020-08-27
OS:	Linux, Windows, Chrome, Mac
Pri:	2
Type:	Bug-Security

Security_Severity-Low
reward-3000
Security_Impact-Stable
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
external_security_bug
Release-0-M91
CVE-2021-30538

Issue 1115045: CSP frame-src bypass using: window.open + javascript-url + about:srcdoc + doubly-nested-iframe.

Reported by dddl...@gmail.com on Tue, Aug 11, 2020, 7:40 AM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36

Steps to reproduce the problem:
1.use `sudo php -S 0.0.0.0:80` to start a web server, and put the bypass-default-src.html and bypass-script-src.html into the web root directory
2.open http://127.0.0.1/bypass-default-src.html and http://127.0.0.1/bypass-script-src.html in your chrome
3.you will see `default-src 'self'` and `script-src 'self'` have been bypassed

What is the expected behavior?
bypass-default-src.html can not load https://xlab.tencent.com
bypass-script-src.html can not load http://d1iv3.me/test.js

What went wrong?
CSP inheritance mechanism error

Did this work before? N/A

Chrome version: 84.0.4147.125 Channel: stable
OS Version: OS X 10.15.6
Flash Version:

bypass-default-src.html
269 bytes View Download

bypass-script-src.html
262 bytes View Download

Comment 1 by dddl...@gmail.com on Tue, Aug 11, 2020, 7:47 AM EDT

what's more object-src, child-src, img-src related policies can also be bypassed, here we just use default-src and script-src as examples

Comment 2 by vakh@chromium.org on Wed, Aug 12, 2020, 8:13 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: mkwst@chromium.org
Labels: Security_Severity-Low Security_Impact-Stable
Components: Blink>SecurityFeature>ContentSecurityPolicy

It appears to me that this is not a bug, it is working as intended.

The description of 'unsafe-inline' states:
Allows the use of inline resources, such as inline <script> elements, javascript: URLs, inline event handlers, and inline <style> elements.

Both POCs here rely on the use of javascript: to load remote resources.

Assigning to mkwst@ to confirm. Adding Security_Severity-Low out of an abundance of caution.

Comment 3 by vakh@chromium.org on Wed, Aug 12, 2020, 8:13 PM EDT Project Member

Labels: OS-Chrome OS-Linux OS-Windows

Comment 4 by dddl...@gmail.com on Wed, Aug 12, 2020, 11:47 PM EDT

I need to emphasize that the CSPs that are bypassed in the POC are default-src and script-src, not unsafe-inline.
The iframe src and script src in the iframe srcdoc needed to follow the default-src'self' and script-src'self', but in this issue they didn't.

If you don't know what went wrong, you can refer to the behavior of Safari and Firefox.

What's more, i think this issue should be **Security_Severity-Medium**

Comment 5 by dddl...@gmail.com on Thu, Aug 13, 2020, 12:33 AM EDT

And as you said, "Both POCs here rely on the use of javascript: to load remote resources.", and javascript: can be executed because of unsafe-line.

I can give you an example (unsafe-inline.html) to explain why unsafe inline javascript cannot load remote resources when default-src 'none' is enabled.

You can compare `bypass-default-src-none.html` and `unsafe-inline.html` in the attachments

unsafe-inline.html
238 bytes View Download

bypass-default-src-none.html
269 bytes View Download

Comment 6 by mkwst@chromium.org on Thu, Aug 13, 2020, 3:09 AM EDT Project Member

Owner: arthu...@chromium.org
Cc: antoniosartori@chromium.org

Does this reproduce in Canary?

arthursonzogni@ has made some recent changes in this area.

Comment 7 by dddl...@gmail.com on Thu, Aug 13, 2020, 3:13 AM EDT

I can reproduce this issue in Canary. The version of my Canary: 86.0.4231.0 canary (x86_64)

Comment 8 by dddl...@gmail.com on Mon, Aug 17, 2020, 11:43 AM EDT

any progress?

Comment 9 by arthu...@chromium.org on Mon, Aug 17, 2020, 12:25 PM EDT Project Member

Summary: CSP frame-src bypass using: window.open + javascript-url + about:srcdoc + doubly-nested-iframe. (was: Chrome Content Security Policy Bypass)
Cc: mkwst@chromium.org clamy@chromium.org
NextAction: 2020-08-27

I confirm. I tried on M84 and M86.
I got two different results, both wrong.

I also tried variations:
1) default-src 'self'
2) default-src 'none'
3) frame-src 'self'
4) frame-src 'none'

but got the same wrong results. It seems the frame-src directive isn't enforced.
I am guessing the sequence: window.open + execute javascript-URL + srcdoc + loading a doubly nested iframe, was enough to confuse the implementation somehow.

I won't have time before the M86 branch cut to investigate more. We need to take another look next week.

Screenshot from 2020-08-17 18-14-40.png
222 KB View Download

Comment 10 by monor...@bugs.chromium.org on Thu, Aug 27, 2020, 8:00 AM EDT

The NextAction date has arrived: 2020-08-27

Comment 11 by dddl...@gmail.com on Mon, Aug 31, 2020, 10:46 PM EDT

any progress? I have tested the POC on Canary 87.0.4250.0 (which is the latest version), it still works (bypassed the CSP successfully)

chrome_canary_87.png
82.1 KB View Download

Comment 12 by arthu...@chromium.org on Wed, Sep 2, 2020, 6:26 AM EDT Project Member

Cc: pmeuleman@chromium.org

pmeuleman@ and antoniosartori@ are going to improve how a given policy, like
CSP, are inherited across documents/navigations. (PolicyContainer)

There are many CSP bugs around inheritance below:
- ~~bug 1117687~~
- ~~bug 1115628~~
- ~~bug 1115208~~
- ~~bug 1115045~~
- ~~bug 1109167~~
- ~~bug 971231~~
- ~~bug 957606~~

I believe their future work might fix several issues in this list.

Comment 13 by dddl...@gmail.com on Mon, Oct 12, 2020, 8:09 AM EDT

Hi, any progress?

Comment 14 by arthu...@chromium.org on Tue, Oct 13, 2020, 3:45 AM EDT Project Member

> Hi, any progress?

A lot of progress.
antoniosartori@ and pmeuleman@ are working on "defining" properly how things in general are inherited toward new documents with a local scheme (about:, data:, javascript:, ...)

This will fix all the issues with CSP. Moreover this isn't limited to CSP as it will also contains several other properties.
Doing the right thing takes times. This won't be fixed in weeks, but months.

Comment 15 by sheriffbot on Fri, Oct 30, 2020, 6:46 PM EDT Project Member

Labels: reward-potential

Comment 16 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 17 by antoniosartori@chromium.org on Thu, Mar 4, 2021, 11:13 AM EST Project Member

Status: Started (was: Assigned)
Owner: antoniosartori@chromium.org

Comment 18 by antoniosartori@chromium.org on Thu, Mar 4, 2021, 11:13 AM EST Project Member

Status: Fixed (was: Started)

This has been fixed by this CL https://chromium-review.googlesource.com/c/chromium/src/+/2667858

Regression test here https://chromium-review.googlesource.com/c/chromium/src/+/2725520

Comment 19 by sheriffbot on Thu, Mar 4, 2021, 12:40 PM EST Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Thu, Mar 4, 2021, 1:55 PM EST Project Member

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

Comment 21 by dddl...@gmail.com on Thu, Mar 4, 2021, 10:51 PM EST

Should this issue be Security_Severity-Medium?

Comment 22 by Git Watcher on Fri, Mar 5, 2021, 5:38 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d2cb713d42b11273c00e57fcf91b25022b387abb

commit d2cb713d42b11273c00e57fcf91b25022b387abb
Author: Antonio Sartori <antoniosartori@chromium.org>
Date: Fri Mar 05 10:36:57 2021

CSP: Add WPT for nested inheritance

This CL adds a Web Platform Test for an edge case of multiple
Content-Security-Policy inheritance for a nested iframe.

~~Bug: 1115015,1149272~~
Change-Id: I492408b8c0f7a3e6cd7dc7e74769c9c8876a34ed
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2725520
Commit-Queue: Antonio Sartori <antoniosartori@chromium.org>
Reviewed-by: Mike West <mkwst@chromium.org>
Reviewed-by: Arthur Sonzogni <arthursonzogni@chromium.org>
Cr-Commit-Position: refs/heads/master@{#860179}

[add] https://crrev.com/d2cb713d42b11273c00e57fcf91b25022b387abb/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/javascript-url-srcdoc-cross-origin-iframe-inheritance.html
[add] https://crrev.com/d2cb713d42b11273c00e57fcf91b25022b387abb/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/support/javascript-url-srcdoc-cross-origin-iframe-inheritance-helper.sub.html
[add] https://crrev.com/d2cb713d42b11273c00e57fcf91b25022b387abb/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/support/postmessage-top.html

Comment 23 by sheriffbot on Wed, Mar 10, 2021, 8:04 PM EST Project Member

Labels: reward-potential

Comment 24 by zhangtiff@google.com on Wed, Mar 17, 2021, 7:12 PM EDT Project Member

Labels: -reward-potential external_security_bug

Comment 25 by amyressler@google.com on Wed, Mar 31, 2021, 6:20 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 26 by amyressler@google.com on Wed, Mar 31, 2021, 6:52 PM EDT Project Member

Congratulations, dddliv3@! The VRP Panel has decided to award you $3000 for this report. A member of our finance team will be in touch soon to arrange payment. In the meantime, please let me know how you would like to be credited for this issue (name/handle you'd like us to use) in the release notes. Nice work!

Comment 27 by dddl...@gmail.com on Thu, Apr 1, 2021, 3:37 AM EDT

Thanks for the bounty!

My credit info: Tianze Ding (@D1iv3) of Tencent Security Xuanwu Lab

Comment 28 by amyressler@google.com on Fri, Apr 2, 2021, 12:12 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 29 by amyressler@chromium.org on Mon, May 24, 2021, 11:30 AM EDT Project Member

Labels: Release-0-M91

Comment 30 by amyressler@google.com on Mon, May 24, 2021, 2:19 PM EDT Project Member

Labels: CVE-2021-30538 CVE_description-missing

Comment 31 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Thu, Jun 24, 2021, 1:54 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