Starred by 1 user

Owner:	caseq@chromium.org
CC:	adetaylor@chromium.org solomonkinard@chromium.org tjudkins@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions
Modified:	Jul 25, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	2
Type:	Bug-Security

Hotlist-Merge-Review
reward-0
Security_Severity-Low
Security_Impact-Stable
allpublic
CVE_description-submitted
Target-78
Target-79
Target-80
M-81
Target-81
Merge-Rejected-83
Release-0-M84
CVE-2020-6530

Issue 1016278: Security: EXC_BAD_ACCESS / KERN_INVALID_ADDRESS when exec chrome.debugger.sendCommand

Reported by myvy...@gmail.com on Mon, Oct 21, 2019, 7:55 AM EDT

Code

VULNERABILITY DETAILS

when chromium extension run `chrome.debugger.sendCommand`, crash with:

Crash reason: EXC_BAD_ACCESS / KERN_INVALID_ADDRESS
Crash address: 0x8

VERSION

Chrome Version: [77.0.3865.120] + stable
Operating System: 10.13.6 (17G6030)

REPRODUCTION CASE

1. load the extension in developer mode, and enable it.
2. open any website, like https://bing.com.
3. click the icon of the extension. crashed.

the extension is modify from live-headers example. only add one line in headers.js:

https://developer.chrome.com/extensions/samples#search:debugger

```
function onEvent(debuggeeId, message, params) {
  if (tabId != debuggeeId.tabId)
    return;

  if (message == "Network.requestWillBeSent") {
    ...
    ...
  } else if (message == "Network.responseReceived") {
    appendResponse(params.requestId, params.response);
+    r = chrome.debugger.sendCommand(
+      {tabId:tabId},
+      "Fetch.getResponseBody",
+      {requestId: params.requestId});
  }
}
```

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: browser
Crash State:
Operating system: Mac OS X

10.13.6 17G6030
CPU: amd64
family 6 model 158 stepping 9
8 CPUs

GPU: UNKNOWN

Crash reason: EXC_BAD_ACCESS / KERN_INVALID_ADDRESS
Crash address: 0x8
Process uptime: 25 seconds

Thread 0 (crashed)
0 Google Chrome Framework + 0xd771d9
rax = 0x00007ffee11e9dd0 rdx = 0x000000011618c058
rcx = 0x000000000000026d rbx = 0x0000000000000000
rsi = 0x000000011618b649 rdi = 0x000000010f8271d9
rbp = 0x00007ffee11e9e20 rsp = 0x00007ffee11e9dd0
r8 = 0x00000000bb61cfb3 r9 = 0x0000000000000005
r10 = 0x8000000000000060 r11 = 0x0000000000000202
r12 = 0x00007ffee11e9e30 r13 = 0x00007ffee11e9fa0
r14 = 0x00007ffee11e9dd0 r15 = 0x00007ffee11e9ea0
rip = 0x000000010f8271d9
Found by: given as instruction pointer in context
1 Google Chrome Framework + 0xd8bd49
rbp = 0x00007ffee11e9e50 rsp = 0x00007ffee11e9e30
rip = 0x000000010f83bd49
Found by: previous frame's frame pointer

CREDIT INFORMATION
Reporter credit: myvyang

live-headers.zip
3.3 KB Download

Comment 1 by carlosil@chromium.org on Mon, Oct 21, 2019, 4:35 PM EDT Project Member

Labels: Security_Impact-Stable M-77 Security_Severity-Medium OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Platform>Extensions

Assigning Medium severity as per https://chromium.googlesource.com/chromium/src/+/master/docs/security/severity-guidelines.md since this requires an extension to be installed

Comment 2 by carlosil@chromium.org on Mon, Oct 21, 2019, 4:36 PM EDT Project Member

Owner: caseq@chromium.org

caseq: Can you PTAL and help find an appropriate owner for this? Thanks.

Comment 3 by carlosil@chromium.org on Mon, Oct 21, 2019, 7:17 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 4 by sheriffbot@chromium.org on Tue, Oct 22, 2019, 10:23 AM EDT Project Member

Labels: Pri-1

Setting Pri-1 to match security severity Medium. 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 5 by sheriffbot@chromium.org on Wed, Oct 23, 2019, 9:10 AM EDT Project Member

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

Comment 6 by sheriffbot@chromium.org on Mon, Nov 4, 2019, 9:10 AM EST Project Member

caseq: 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 7 by sheriffbot@chromium.org on Mon, Nov 18, 2019, 9:10 AM EST Project Member

caseq: Uh oh! This issue still open and hasn't been updated in the last 28 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 8 by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:11 AM EST Project Member

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

Comment 9 by sheriffbot@chromium.org on Wed, Feb 5, 2020, 10:47 AM EST Project Member

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

Comment 10 by sheriffbot on Thu, Apr 9, 2020, 12:29 PM EDT Project Member

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

Comment 11 by bugdroid on Fri, Apr 17, 2020, 8:09 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/d4938b0019bc23f96e2c7d3659c0a4102973d8c2

commit d4938b0019bc23f96e2c7d3659c0a4102973d8c2
Author: Andrey Kosyakov <caseq@chromium.org>

Date: Sat Apr 18 00:07:39 2020

DevTools: check whether Fetch domain is enabled before handling commands

~~Bug: 1016278~~
Change-Id: Icd80e3b287f090ffb4ac67437e7e1ebae392c98b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2154228
Reviewed-by: Peter Kvitek <kvitekp@chromium.org>
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Cr-Commit-Position: refs/heads/master@{#760266}

[modify] https://crrev.com/d4938b0019bc23f96e2c7d3659c0a4102973d8c2/content/browser/devtools/protocol/fetch_handler.cc
[add] https://crrev.com/d4938b0019bc23f96e2c7d3659c0a4102973d8c2/third_party/blink/web_tests/http/tests/inspector-protocol/fetch/calls-while-not-enabled-expected.txt
[add] https://crrev.com/d4938b0019bc23f96e2c7d3659c0a4102973d8c2/third_party/blink/web_tests/http/tests/inspector-protocol/fetch/calls-while-not-enabled.js

Comment 12 by caseq@chromium.org on Sat, Apr 18, 2020, 1:32 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 13 by sheriffbot on Sat, Apr 18, 2020, 3:04 PM EDT Project Member

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

Comment 14 by natashapabrai@google.com on Mon, Apr 20, 2020, 3:46 PM EDT Project Member

Labels: reward-topanel

Comment 15 by sheriffbot on Tue, Apr 21, 2020, 3:26 PM EDT Project Member

Labels: Merge-Request-83

Requesting merge to beta M83 because latest trunk commit (760266) appears to be after beta branch point (756066).

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

Comment 16 by sheriffbot on Tue, Apr 21, 2020, 3:30 PM EDT Project Member

Labels: -Merge-Request-83 Merge-Review-83 Hotlist-Merge-Review

This bug requires manual review: To minimize risk and increase branch stability, all merge requests are being reviewed manually by the release team.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), cindyb@(ChromeOS), srinivassista@(Desktop)

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

Comment 17 by srinivassista@google.com on Wed, Apr 22, 2020, 2:15 PM EDT Project Member

Cc: adetaylor@chromium.org

+adetaylor@ to review/approve

caseq@ please answer questions in comment #16

Comment 18 by adetaylor@google.com on Wed, Apr 22, 2020, 5:03 PM EDT Project Member

caseq@ please more generally comment on whether you consider the change at all risky. It looks extremely straightforward to me.

Comment 19 by caseq@chromium.org on Wed, Apr 22, 2020, 5:04 PM EDT Project Member

1. yes at this stage. in general, I think this should be treated as a stability bug rather than security one (this is just an NPE).
2. See above.
3. Yes.
4. Stability fix.
5. No
6. This is not a feature.

Comment 20 by adetaylor@chromium.org on Wed, Apr 22, 2020, 6:08 PM EDT Project Member

Labels: -Security_Severity-Medium -Merge-Review-83 Merge-Rejected-83 Security_Severity-Low

OK, if this is an NPE, this is probably not a security bug at all, but I'll keep it in the security queue just in case the offset is unexpectedly controllable. I don't want to merge this back though. Thanks for the answers!

Comment 21 by natashapabrai@google.com on Wed, Apr 22, 2020, 9:39 PM EDT Project Member

Labels: -reward-topanel reward-0

Unfortunately the Panel declined to award this report.

Comment 22 by sheriffbot on Thu, Apr 23, 2020, 2:46 PM EDT Project Member

Labels: -Pri-1 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 23 by adetaylor@google.com on Sun, Jul 12, 2020, 10:15 PM EDT Project Member

Labels: Release-0-M84

Comment 24 by adetaylor@chromium.org on Mon, Jul 13, 2020, 2:08 PM EDT Project Member

Labels: CVE-2020-6530 CVE_description-missing

Comment 25 by adetaylor@google.com on Wed, Jul 22, 2020, 12:14 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 26 by sheriffbot on Sat, Jul 25, 2020, 3:06 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