☆ Starred by 5 users

Owner:	a...@chromium.org
CC:	lazyboy@chromium.org est...@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>WebAppInstalls>ProtocolHandling
Modified:	Oct 20, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-20000
CVE_description-submitted
M-91
Target-91
external_security_report
merge-merged-4430
merge-merged-90
FoundIn-91
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
Release-0-M92
CVE-2021-30574
LTS-Size-Small
LTS-Complexity-Minimal

Issue 1227315: Security: HeapOverflow in ProtocolHandler

Reported by leecraso@gmail.com on Thu, Jul 8, 2021, 4:00 AM EDT

Code

VULNERABILITY DETAILS
Unregistering protocol handler after ContextMenu popup could make the size of vector handlers[1] mismatch the actual number of handlers showed in ContextMenu. So the HeapOverflow could be triggered when the selected handle index[2] is greater than the vector size.

[1].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/renderer_context_menu/render_view_context_menu.cc;l=2994;drc=02646205f1ddd401162942b14f736533ab2cc87f
[2].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/renderer_context_menu/render_view_context_menu.cc;l=3003;drc=02646205f1ddd401162942b14f736533ab2cc87f

VERSION
Chrome Version: stable
Operating System: All

REPRODUCTION CASE

```
$ python -m SimpleHTTPServer
$ out/asan/chrome --user-data-dir=/tmp/xxxx "http://localhost:8000/poc.html"
```

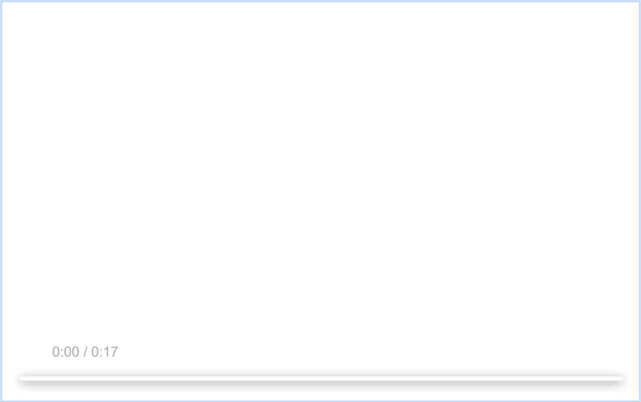
Click "Register" button, right-click the email link and open link with the second handle.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State: see asan file

CREDIT INFORMATION
Reporter credit: Leecraso and Guang Gong of 360 Alpha Lab

asan
14.0 KB View Download

Demo.mp4
1.5 MB View Download



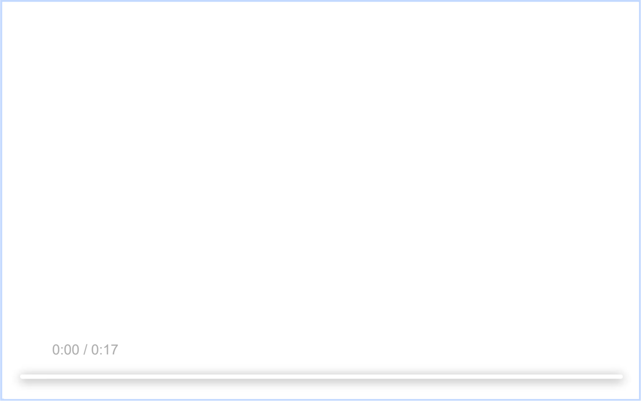
poc.html
589 bytes View Download

Comment 1 by sheriffbot on Thu, Jul 8, 2021, 4:01 AM EDT Project Member
Labels: external_security_report

Comment 2 by leecraso@gmail.com on Thu, Jul 8, 2021, 4:01 AM EDT
In chromeOS, there is already a pre-registered protocol handler. Therefore, for other platforms, you need to use this poc to register two protocol handlers from different origins.

asan
11.1 KB View Download

Demo.mp4
1.5 MB View Download



poc.html
757 bytes View Download

iframe.html
349 bytes View Download

Comment 3 by rsesek@chromium.org on Thu, Jul 8, 2021, 3:54 PM EDT Project Member
Status: Assigned (was: Unconfirmed)
Owner: a...@chromium.org
Cc: lazyboy@chromium.org
Labels: FoundIn-91 Security_Severity-High OS-Linux Pri-1
Components: UI>Browser>WebAppInstalls>ProtocolHandling

Thanks I can reproduce this on Linux using ASan-release. Some more detailed steps from Linux:

1) Navigate to the POC that is served on a HTTPS or local HTTP server
2) Press the Register button
3) Right click the email link
4) Wait 1 second
5) Click Open link with… > {domain}

Comment 4 by sheriffbot on Thu, Jul 8, 2021, 3:57 PM EDT Project Member
Labels: Security_Impact-Stable

Comment 5 by a...@chromium.org on Thu, Jul 8, 2021, 6:37 PM EDT Project Member
ProtocolHandlerRegistry has a single observation callback that the handlers have changed, so invalidating the handler list is the simplest fix.

I stalled out in test writing because there's no good way to fake out protocol handlers, nor their registry, nor menus. Going to upload the fix.

Comment 6 by sheriffbot on Fri, Jul 9, 2021, 12:46 PM EDT Project Member
Labels: M-91 Target-91

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 7 by Git Watcher on Fri, Jul 9, 2021, 3:45 PM EDT Project Member
The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2738faaac807b46e8df16ddff8b60489aa816c40

commit 2738faaac807b46e8df16ddff8b60489aa816c40

Author: Avi Drissman <avi@chromium.org>
Date: Fri Jul 09 19:44:02 2021

Don't call through a protocol handler if they've changed

Have any protocol handler change invalidate the list of protocol
handlers in the context menu.

~~Bug: 1227315~~
Change-Id: Iab8e475454cd946f153102111b02f73de24648fb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3017137
Commit-Queue: Robert Sesek <rsesek@chromium.org>
Auto-Submit: Avi Drissman <avi@chromium.org>
Reviewed-by: Robert Sesek <rsesek@chromium.org>
Cr-Commit-Position: refs/heads/master@{#900104}

[modify] https://crrev.com/2738faaac807b46e8df16ddff8b60489aa816c40/chrome/browser/renderer_context_menu/render_view_context_menu.cc
[modify] https://crrev.com/2738faaac807b46e8df16ddff8b60489aa816c40/chrome/browser/renderer_context_menu/render_view_context_menu.h

Comment 8 by a...@chromium.org on Fri, Jul 9, 2021, 3:50 PM EDT Project Member

Fix landed in 93. How far back to merge?

Comment 9 by a...@chromium.org on Fri, Jul 9, 2021, 3:51 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 10 by sheriffbot on Sat, Jul 10, 2021, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 11 by sheriffbot on Sat, Jul 10, 2021, 2:00 PM EDT Project Member

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

Comment 12 by sheriffbot on Sat, Jul 10, 2021, 2:20 PM EDT Project Member

Labels: Merge-Request-92 Merge-Request-91

Requesting merge to stable M91 because latest trunk commit (900104) appears to be after stable branch point (870763).

Requesting merge to beta M92 because latest trunk commit (900104) appears to be after beta branch point (885287).

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

Comment 13 by sheriffbot on Sat, Jul 10, 2021, 2:25 PM EDT Project Member

Labels: -Merge-Request-92 Merge-Review-92 Hotlist-Merge-Review

This bug requires manual review: We are only 9 days from stable.
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/+/main/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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

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

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

Comment 14 by a...@chromium.org on Sat, Jul 10, 2021, 8:28 PM EDT Project Member

1. Yes; it's a security bug.
2. https://crrev.com/c/3017137
3. Yes.
4. Yes; 91 and 92
5. Security.
6. No
7. n/a

Comment 15 by joenotcharles@google.com on Sun, Jul 11, 2021, 8:45 AM EDT Project Member

Owner: joenotcharles@google.com

I'll do the merge while avi's OOO

Comment 16 by adetaylor@google.com on Tue, Jul 13, 2021, 1:34 PM EDT Project Member

Labels: -Merge-Review-92 Merge-Approved-92

Approving merge to M92, branch 4515.

Comment 17 by Git Watcher on Tue, Jul 13, 2021, 3:47 PM EDT Project Member

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/42a7279960cc97a1916daeffd7f1683db0e00db2

commit 42a7279960cc97a1916daeffd7f1683db0e00db2
Author: Avi Drissman <avi@chromium.org>
Date: Tue Jul 13 19:46:21 2021

Don't call through a protocol handler if they've changed

Have any protocol handler change invalidate the list of protocol
handlers in the context menu.

(cherry picked from commit 2738faaac807b46e8df16ddff8b60489aa816c40)

~~Bug: 1227315~~

Change-Id: Iab8e475454cd946f153102111b02f73de24648fb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3017137
Commit-Queue: Robert Sesek <rsesek@chromium.org>
Auto-Submit: Avi Drissman <avi@chromium.org>
Reviewed-by: Robert Sesek <rsesek@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#900104}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3024592
Commit-Queue: Joe Mason <joenotcharles@chromium.org>
Commit-Queue: Istiaque Ahmed <lazyboy@chromium.org>
Auto-Submit: Joe Mason <joenotcharles@chromium.org>
Reviewed-by: Istiaque Ahmed <lazyboy@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#1525}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/42a7279960cc97a1916daeffd7f1683db0e00db2/chrome/browser/renderer_context_menu/render_view_context_menu.cc
[modify] https://crrev.com/42a7279960cc97a1916daeffd7f1683db0e00db2/chrome/browser/renderer_context_menu/render_view_context_menu.h

Comment 18 by joenotcharles@google.com on Fri, Jul 16, 2021, 12:18 PM EDT Project Member

Owner: a...@chromium.org

Now I'm going OOO but I think avi will be back next week, so back to you to do the M91 merge once it's approved.

Comment 19 by amyressler@chromium.org on Mon, Jul 19, 2021, 3:02 PM EDT Project Member

Labels: Release-0-M92

Comment 20 by amyressler@google.com on Mon, Jul 19, 2021, 7:16 PM EDT Project Member

Labels: CVE-2021-30574 CVE_description-missing

Comment 21 by rzanoni@google.com on Tue, Jul 20, 2021, 10:34 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 22 by rzanoni@google.com on Wed, Jul 21, 2021, 7:58 AM EDT Project Member

Labels: LTS-Size-Small LTS-Complexity-Minimal

Comment 23 by amyressler@google.com on Thu, Jul 22, 2021, 1:06 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-20000

*** 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 24 by amyressler@google.com on Thu, Jul 22, 2021, 1:21 PM EDT Project Member

Congratulations, Leecraso and Guang Gong! The VRP Panel has decided to award you $20,000 for this report. Nice work!

Comment 25 by amyressler@google.com on Fri, Jul 23, 2021, 5:53 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 26 by gianluca@google.com on Tue, Jul 27, 2021, 10:36 AM EDT Project Member

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 27 by amyressler@google.com on Tue, Jul 27, 2021, 5:58 PM EDT Project Member

Labels: -Merge-Request-91 Merge-Approved-91

Hello avi, (assuming you are back :)) please go ahead and merge this to M91, branch 4472 at your earliest convenience, so this can be a part of the extended stable channel release branch. Thank you!

Comment 28 by Git Watcher on Wed, Jul 28, 2021, 4:58 AM EDT Project Member

Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c722a52c34e805e68671dc43a47dbf3980beb6da

commit c722a52c34e805e68671dc43a47dbf3980beb6da
Author: Roger Zanoni <rzanoni@google.com>
Date: Wed Jul 28 08:57:56 2021

[M90-LTS] Don't call through a protocol handler if they've changed

Have any protocol handler change invalidate the list of protocol
handlers in the context menu.

(cherry picked from commit 2738faaac807b46e8df16ddff8b60489aa816c40)

~~Bug: 1227315~~
Change-Id: Iab8e475454cd946f153102111b02f73de24648fb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3017137
Commit-Queue: Robert Sesek <rsesek@chromium.org>
Auto-Submit: Avi Drissman <avi@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#900104}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3041344
Owners-Override: Jana Grill <janagrill@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1543}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/c722a52c34e805e68671dc43a47dbf3980beb6da/chrome/browser/renderer_context_menu/render_view_context_menu.cc
[modify] https://crrev.com/c722a52c34e805e68671dc43a47dbf3980beb6da/chrome/browser/renderer_context_menu/render_view_context_menu.h

Comment 29 by rzanoni@google.com on Wed, Jul 28, 2021, 5:43 AM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 30 by Git Watcher on Wed, Jul 28, 2021, 11:44 AM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/27e1ef2dedcc28b167e1c283829d4d55935628ed

commit 27e1ef2dedcc28b167e1c283829d4d55935628ed
Author: Avi Drissman <avi@chromium.org>
Date: Wed Jul 28 15:43:22 2021

[M91 Merge] Don't call through a protocol handler if they've changed

Have any protocol handler change invalidate the list of protocol
handlers in the context menu.

(cherry picked from commit 2738faaac807b46e8df16ddff8b60489aa816c40)

~~Bug: 1227315~~
Change-Id: I1c5c6197659f7f321e97197ff4070a16191829dc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3017137
Commit-Queue: Robert Sesek <rsesek@chromium.org>
Auto-Submit: Avi Drissman <avi@chromium.org>
Reviewed-by: Robert Sesek <rsesek@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#900104}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057890
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#1585}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/27e1ef2dedcc28b167e1c283829d4d55935628ed/chrome/browser/renderer_context_menu/render_view_context_menu.cc
[modify] https://crrev.com/27e1ef2dedcc28b167e1c283829d4d55935628ed/chrome/browser/renderer_context_menu/render_view_context_menu.h

Comment 31 by amyressler@google.com on Tue, Aug 3, 2021, 3:41 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Wed, Oct 20, 2021, 1:30 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