Starred by 3 users

Owner:	est...@chromium.org
CC:	----
Status:	Fixed *(Closed)*
Components:	UI>Browser>NewTabPage
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
FoundIn-75
external_security_report
M-99
Target-99
Security_Impact-Extended
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0980

Issue 1302157: Security: Heap-use-after-free in ~ExtensionUninstallDialogViews

Reported by merc....@gmail.com on Tue, Mar 1, 2022, 8:58 PM EST

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

Steps to reproduce the problem:
1. download asan-linux-release-976045.zip and unzip
2. install the extension
3. open 'chrome://apps', select to remove the apps
4. close the 'chrome://apps' tab by the Dock. See the video for more informations.

What is the expected behavior?

What went wrong?
When close the chrome://apps, the `AppLauncherHandler` will be destructed first, then the `ExtensionUninstallDialog` will be destructed. But `ExtensionUninstallDialog` hold a raw ptr to `AppLauncherHandler`, the `extensions::ExtensionUninstallDialog::Delegate`[1]. So when `ExtensionUninstallDialog` is destructed, UAF occurs.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/extensions/extension_uninstall_dialog.h;l=163;bpv=1;bpt=0;drc=9e30513cb5818b899ef42ad3a9f26eb2dabdffc9

Did this work before? N/A

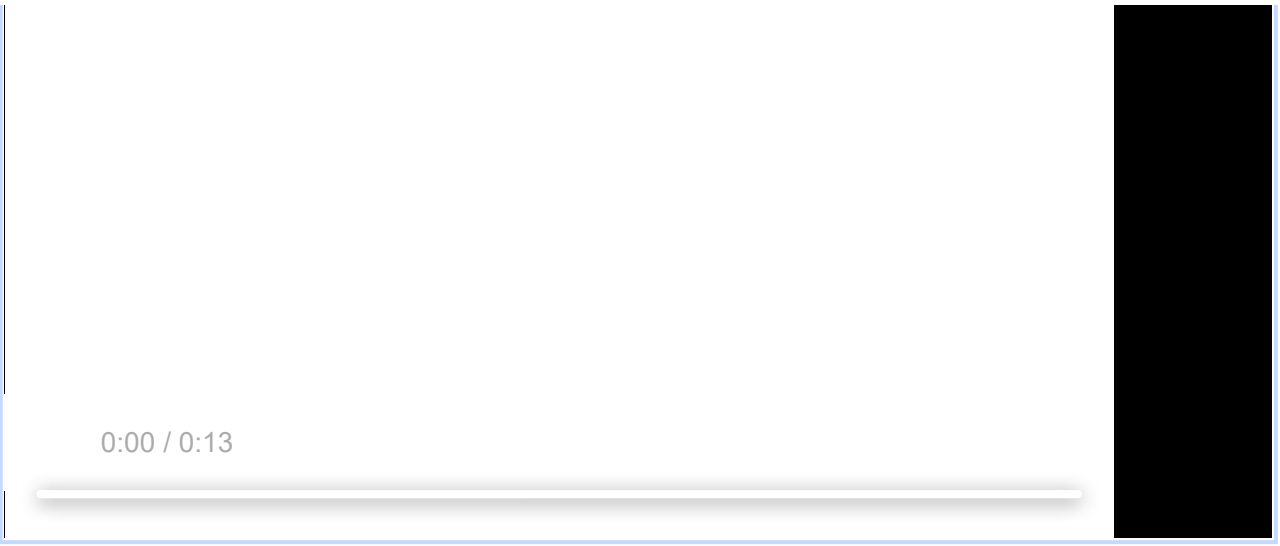
Chrome version: 98.0.4758.102 Channel: n/a
OS Version:

background.js
NaN MB View Download

manifest.json
227 bytes View Download

asan.txt
24.8 KB View Download

video.webm
548 KB View Download



Comment 1 by sheriffbot on Tue, Mar 1, 2022, 9:02 PM EST Project Member

Labels: external_security_report

Comment 2 by dcheng@chromium.org on Wed, Mar 2, 2022, 2:22 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: est...@chromium.org
Labels: Security_Severity-Medium FoundIn-75 Pri-1
Components: UI>Browser>NewTabPage

Simple "fix" is probably to move `std::unique_ptr<extensions::ExtensionUninstallDialog> extension_uninstall_dialog_` to be the last field with a comment that it calls back into `this`.

It's a bit sketchy of course :)

While this is a UaF in the browser, I think it'd be difficult to exploit in practice, so I'm going to label this as medium.

Comment 3 by sheriffbot on Wed, Mar 2, 2022, 2:26 AM EST Project Member

Labels: Security_Impact-Extended

Comment 4 by sheriffbot on Wed, Mar 2, 2022, 12:52 PM EST Project Member

Labels: M-99 Target-99

Setting milestone and target because of medium severity.

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

Comment 5 by Git Watcher on Thu, Mar 3, 2022, 2:21 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/64f02e6e38d192a234a1d4f873d01e05aa85a367

commit 64f02e6e38d192a234a1d4f873d01e05aa85a367

Author: Evan Stade <estade@chromium.org>
Date: Thu Mar 03 07:20:05 2022

Fix UAF in apps page.

~~Bug: 1302157~~
Change-Id: I078d20add15bccec84ba13c384c191fd3b60c85b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3498946
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Evan Stade <estade@chromium.org>
Cr-Commit-Position: refs/heads/main@{#977002}

[modify]
https://crrev.com/64f02e6e38d192a234a1d4f873d01e05aa85a367/chrome/browser/ui/webui/ntp/app_launcher_handler.cc
[modify]
https://crrev.com/64f02e6e38d192a234a1d4f873d01e05aa85a367/chrome/browser/ui/webui/ntp/app_launcher_handler.h
[modify]
https://crrev.com/64f02e6e38d192a234a1d4f873d01e05aa85a367/chrome/browser/ui/webui/ntp/app_launcher_handler_unittest.cc

Comment 6 by est...@chromium.org on Fri, Mar 4, 2022, 8:23 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 7 by sheriffbot on Sat, Mar 5, 2022, 12:41 PM EST Project Member

Labels: reward-topanel

Comment 8 by sheriffbot on Sat, Mar 5, 2022, 1:40 PM EST Project Member

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

Comment 9 by est...@chromium.org on Mon, Mar 7, 2022, 10:42 AM EST Project Member

Status: Started (was: Fixed)
Labels: Merge-Request-99

based on labels I'm guessing we want to cherry pick the fix back to 99?

Comment 10 by sheriffbot on Mon, Mar 7, 2022, 10:45 AM EST Project Member

Labels: -Merge-Request-99 Hotlist-Merge-Review Merge-Review-99

Merge review required: M99 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), cah (ChromeOS), pbommana (Desktop)

Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), ppommana (Desktop)

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

Comment 11 by est...@chromium.org on Mon, Mar 7, 2022, 11:01 AM EST Project Member

Labels: OS-Mac OS-Windows

1. Why does your merge fit within the merge criteria for these milestones?

medium security bug

2. What changes specifically would you like to merge? Please link to Gerrit.

https://chromium-review.googlesource.com/c/chromium/src/+/3498946

3. Have the changes been released and tested on canary?

yes

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?

no

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents

non cros bug

6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

no

Comment 12 by est...@chromium.org on Mon, Mar 7, 2022, 11:21 AM EST Project Member

(manually tested with asan-linux-release-977999)

Comment 13 by amyressler@chromium.org on Mon, Mar 7, 2022, 1:19 PM EST Project Member

Status: Fixed (was: Started)

Comment 14 by amyressler@chromium.org on Mon, Mar 7, 2022, 1:23 PM EST Project Member

Labels: Merge-Review-100

Hi estade@ thanks for landing this fix. Yes, we'll want to CP this to M99, but also to M100 since it was landed on canary and dev past 100 branching. In the future, once you've resolved a security bug, please update as Fixed immediately upon submitting the fix CL and sheriffbot will update with appropriate merge labels accordingly

Comment 15 by amyressler@chromium.org on Mon, Mar 7, 2022, 1:30 PM EST Project Member

Labels: -Merge-Review-100 Merge-Approved-100

merge approved to M100, please merge to branch 4896 at your earliest convenience
merge approved to M99, please merge to branch 4844 NLT noon PST, Thursday 10 March so this fix can be included in the next stable respin... thank you!

next stable respin -- thank you!

Comment 16 by amyressler@chromium.org on Mon, Mar 7, 2022, 1:31 PM EST Project Member

Labels: -Merge-Review-99

Comment 17 by est...@chromium.org on Mon, Mar 7, 2022, 2:31 PM EST Project Member

> In the future, once you've resolved a security bug, please update as Fixed immediately upon submitting the fix CL and sheriffbot will update with appropriate merge labels accordingly

I did this in #c6 and sheriffbot did not mention anything about merging.

Comment 18 by srinivassista@google.com on Mon, Mar 7, 2022, 2:55 PM EST Project Member

This bug is approved for M100 merge, please complete your merge asap so this can be included in the beta release this week. Beta RC will be cut tomorrow (tuesday) March 8th at 3pm PST [Bulk Update]

Comment 19 by Git Watcher on Mon, Mar 7, 2022, 3:51 PM EST Project Member

Labels: -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/db2176c1d001ff4f52026c0920c2393ee24115b7

commit db2176c1d001ff4f52026c0920c2393ee24115b7
Author: Evan Stade <estade@chromium.org>
Date: Mon Mar 07 20:50:22 2022

Fix UAF in apps page.

(cherry picked from commit 64f02e6e38d192a234a1d4f873d01e05aa85a367)

~~Bug: 1302157~~
Change-Id: I078d20add15bccec84ba13c384c191fd3b60c85b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3498946
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Evan Stade <estade@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977002}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508256
Auto-Submit: Evan Stade <estade@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4896@{#349}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/db2176c1d001ff4f52026c0920c2393ee24115b7/chrome/browser/ui/webui/ntp/app_launcher_handler.cc
[modify]
https://crrev.com/db2176c1d001ff4f52026c0920c2393ee24115b7/chrome/browser/ui/webui/ntp/app_launcher_handler.h
[modify]
https://crrev.com/db2176c1d001ff4f52026c0920c2393ee24115b7/chrome/browser/ui/webui/ntp/app_launcher_handler_unittest.cc

Comment 20 by Git Watcher on Mon, Mar 7, 2022, 4:14 PM EST Project Member

Labels: merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e400cb1bdffdc10f87cf648481d3eadf96fd8496

commit e400cb1bdffdc10f87cf648481d3eadf96fd8496
Author: Evan Stade <estade@chromium.org>
Date: Mon Mar 07 21:13:06 2022

Fix UAF in apps page.

(cherry picked from commit 64f02e6e38d192a234a1d4f873d01e05aa85a367)

~~Bug: 1302157~~
Change-Id: I078d20add15bccec84ba13c384c191fd3b60c85b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3498946
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Evan Stade <estade@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977002}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508332
Auto-Submit: Evan Stade <estade@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4844@{#999}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify]
https://crrev.com/e400cb1bdffdc10f87cf648481d3eadf96fd8496/chrome/browser/ui/webui/ntp/app_launcher_handler.cc
[modify]
https://crrev.com/e400cb1bdffdc10f87cf648481d3eadf96fd8496/chrome/browser/ui/webui/ntp/app_launcher_handler.h
[modify]
https://crrev.com/e400cb1bdffdc10f87cf648481d3eadf96fd8496/chrome/browser/ui/webui/ntp/app_launcher_handler_unittest.cc

Comment 21 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:24 PM EST Project Member

Labels: Release-1-M99

Comment 22 by amyressler@chromium.org on Fri, Mar 11, 2022, 4:37 PM EST Project Member

re: comment #17: hi estade@, sheriffbot runs the merge labeling rules every 24 hours at the same time, you were about two hours early from when the bot would have woken up and reported to work :)

Comment 23 by amyressler@google.com on Mon, Mar 14, 2022, 6:14 PM EDT Project Member

Labels: CVE-2022-0980 CVE_description-missing

Comment 24 by amyressler@google.com on Thu, Mar 31, 2022, 5:15 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

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 25 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:42 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $3,000 for this report amount. The Panel assess security impact and exploitation potential and determined this reward amount due to the high reliance on specific and direct user interaction required to trigger this issue. Thank you for your efforts and reporting this issue to us!

Comment 26 by amyressler@google.com on Fri, Apr 1, 2022, 4:06 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 27 by sheriffbot on Tue, Jun 14, 2022, 1:27 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 28 by xpsve...@gmail.com on Wed, Jun 15, 2022, 8:45 AM EDT

Can the attachments in the original report be undeleted?

Comment 29 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 30 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:19 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing