

☆ Starred by 6 users

Owner:

dewittj@chromium.org

CC:


adetaylor@chromium.org

dim...@chromium.org

mvano...@chromium.org

est...@chromium.org

pbomm...@chromium.org

 knollr@chromium.org

dcheng@chromium.org

peter@chromium.org

josa...@google.com

Status:

Fixed (Closed)

Components:

UI>Notifications

Modified:

Aug 19, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Android, Windows, Chrome, Mac

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review

Security_Impact-Stable

Security_Severity-High

allpublic

reward-inprocess

reward-20000

CVE_description-submitted

M-90

Target-90

merge-merged-4240

LTS-Security-86

external_security_report

LTS-Merge-Approved-86

merge-merged-4430

merge-merged-90

merge-merged-4472

merge-merged-91

merge-merged-4430_101

Release-3-M90

CVE-2021-30512

Issue 1200019: Security: heap-buffer-overflow in PlatformNotificationServiceImpl::CreateNotificationFromData

Reported by zhanj...@gmail.com on Sat, Apr 17, 2021, 3:02 AM EDT

 Code

VULNERABILITY DETAILS

https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/notifications/platform_notification_service_impl.cc;l=453;bpv=0;bpt=1

if `notification_data.actions.size()` > `notification_resources.action_icons.size()`, access `notification_resources.action_icons[i]` will cause heap overflow.

tigger this bug need Notification permission.

VERSION

Chrome Version: 92.0.4480.0 [x64 dev]

Operating System: ubuntu20.10

REPRODUCTION CASE

1.python copy_mojo_js_bindings.py path/to/ASAN/gen/

2.python3 -m http.server

3./chrome --enable-blink-features=MojoJS --user-data-dir=/tmp/nonexist <http://localhost:8000/test.html>

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: browser

test.html

2.0 KB [View](#) [Download](#)

[Deleted]

asan.txt

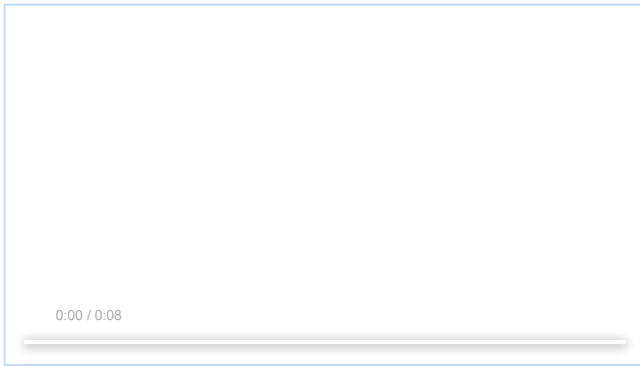
Comment 1 by sheriffbot on Sat, Apr 17, 2021, 3:06 AM EDT Project Member

Labels: external_security_report

Comment 2 by zhanj...@gmail.com on Sat, Apr 17, 2021, 3:42 AM EDT

poc.mp4

1.0 MB [View](#) [Download](#)



Comment 3 by zhanj...@gmail.com on Sat, Apr 17, 2021, 9:11 AM EDT

asan2.txt
15.2 KB [View](#) [Download](#)

Comment 4 by est...@chromium.org on Mon, Apr 19, 2021, 4:49 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: dewittj@chromium.org
Cc: dim...@chromium.org knollr@chromium.org peter@chromium.org
Labels: Security_Severity-High Security_Impact-Stable M-89 OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Notifications

Tentatively triaging as High assuming it's not possible to exploit this without a compromised renderer. (Also, even if it were possible, needing to grant notifications permission might still downgrade to High.)

Notifications owners, could you please take a look?

Comment 5 by est...@chromium.org on Mon, Apr 19, 2021, 4:52 PM EDT Project Member

Cc: mvano...@chromium.org

Comment 6 by dewittj@chromium.org on Mon, Apr 19, 2021, 5:55 PM EDT Project Member

After a quick look, I found that Blink normally populates an action icon image for each notification action, so this would require a compromised renderer.

Comment 7 by dewittj@chromium.org on Mon, Apr 19, 2021, 10:28 PM EDT Project Member

Status: Started (was: Assigned)

CL in review: <https://chromium-review.googlesource.com/c/chromium/src/+2838205>

Comment 8 by sheriffbot on Tue, Apr 20, 2021, 12:21 PM EDT Project Member

Labels: -M-89 M-90 Target-90

Comment 9 by Git Watcher on Fri, Apr 23, 2021, 3:16 PM EDT Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d>

commit 3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d
Author: Justin DeWitt <dewittj@chromium.org>
Date: Fri Apr 23 19:15:56 2021

Notifications: crash if improper action icons sent from renderer.

Previously, the code only called DCHECK but as this data is from a renderer we should probably crash the browser.

~~Bug=1289049~~

Change-Id: If4d9d48c8e18a3ed9c8bb3a50b952591259e0db5
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2838205>
Commit-Queue: Justin DeWitt <dewittj@chromium.org>
Reviewed-by: Peter Beverloo <peter@chromium.org>
Cr-Commit-Position: refs/heads/master@{#875788}

[modify] https://crrev.com/3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d/chrome/browser/notifications/platform_notification_service_impl.cc
[modify] https://crrev.com/3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d/content/browser/notifications/blink_notification_service_impl.cc
[modify] https://crrev.com/3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d/content/browser/notifications/blink_notification_service_impl.h

Comment 10 by dewittj@chromium.org on Fri, Apr 23, 2021, 6:06 PM EDT Project Member

Cc: est...@chromium.org

Emily, after this is verified on Canary, does security team want to merge to M90 or M91?

Comment 11 by est...@chromium.org on Fri, Apr 23, 2021, 8:14 PM EDT Project Member

This is High severity (memory corruption in browser process triggerable from a compromised renderer; see <https://chromium.googlesource.com/chromium/src/+master/docs/security/severity-guidelines.md#TOC-High-severity>) so it should be merged to current stable milestone M90.

Comment 12 by dewittj@chromium.org on Tue, Apr 27, 2021, 7:56 PM EDT Project Member

Labels: Merge-Request-90 Merge-Request-91

Requesting merge. Canary does not see a spike in crashes in %notification_service% so I think this is safe enough.

https://crash.corp.google.com/browse?q=expanded_custom_data.ChromeCrashProto.channel%3D%27canary%27+AND+expanded_custom_data.ChromeCrashProto.magic_signature_1.name+LIKE+%27%25notification_service%25%27#productname:1000,productversion:1020,-processtype,+magicsignature:100,magicsignature2:50,stablename:50,productversionbyos:20,device:1000,day:110,experiments:10000

Comment 13 by sheriffbot on Tue, Apr 27, 2021, 7:59 PM EDT Project Member

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91's targeted beta branch promotion date has already passed, so this requires manual review
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 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: benmason@(Android), bindusuvama@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 14 by [pbommana@google.com](#) on Wed, Apr 28, 2021, 3:45 PM EDT Project Member

Cc: [adetaylor@chromium.org](#) [pbomm...@chromium.org](#)

[dewittj@](#) please reply to the questions posted in [comment#13](#), thank you.

+Adrian(Security TPM)

Comment 15 by [adetaylor@chromium.org](#) on Wed, Apr 28, 2021, 5:39 PM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-91

Please mark it as fixed if it is: <https://chromium.googlesource.com/chromium/src/+master/docs/security/security-labels.md#TOC-Merge-labels> - then the merge process would have kick in automatically.

Assuming this is deemed a complete fix, approving merge to M91, branch 4472. Merges to M90 will be approved at a later date when we've got a release coming up.

Comment 16 by [dewittj@google.com](#) on Wed, Apr 28, 2021, 6:54 PM EDT Project Member

Status: Fixed (was: Started)

#15 - Apologies, this is different from the normal merge process.

Comment 17 by [adetaylor@chromium.org](#) on Wed, Apr 28, 2021, 7:36 PM EDT Project Member

Cc: [josa...@google.com](#)

Comment 18 by [sheriffbot](#) on Thu, Apr 29, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 19 by [sheriffbot](#) on Thu, Apr 29, 2021, 2:02 PM EDT Project Member

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

Comment 20 by [Git Watcher](#) on Thu, Apr 29, 2021, 4:48 PM 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/+cdb8756d339fa80f1f7ad12b46ae9651bc4768d8>

commit [cdb8756d339fa80f1f7ad12b46ae9651bc4768d8](#)

Author: Justin DeWitt <[dewittj@chromium.org](#)>

Date: Thu Apr 29 20:47:08 2021

Notifications: crash if improper action icons sent from renderer.

Previously, the code only called DCHECK but as this data is from a renderer we should probably crash the browser.

(cherry picked from commit [3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d](#))

~~Bug=4200040~~

Change-Id: [If4d9d48c8e18a3ed9c8bb3a50b952591259e0db5](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2838205>

Commit-Queue: Justin DeWitt <[dewittj@chromium.org](#)>

Reviewed-by: Peter Beverloo <[peter@chromium.org](#)>

Cr-Original-Commit-Position: refs/heads/master@{#875788}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2860443>

Owners-Override: Justin DeWitt <[dewittj@chromium.org](#)>

Auto-Submit: Justin DeWitt <[dewittj@chromium.org](#)>

Commit-Queue: Adrian Taylor <[adetaylor@chromium.org](#)>

Reviewed-by: Adrian Taylor <[adetaylor@chromium.org](#)>

Cr-Commit-Position: refs/branch-heads/4472@{#577}

Cr-Branched-From: [3d60439cfb36485e76a1c5bb7f513d3721b20da1](#)-refs/heads/master@{#870763}

[modify] https://crrev.com/cdb8756d339fa80f1f7ad12b46ae9651bc4768d8/chrome/browser/notifications/platform_notification_service_impl.cc

[modify] https://crrev.com/cdb8756d339fa80f1f7ad12b46ae9651bc4768d8/content/browser/notifications/blink_notification_service_impl.cc

[modify] https://crrev.com/cdb8756d339fa80f1f7ad12b46ae9651bc4768d8/content/browser/notifications/blink_notification_service_impl.h

Comment 21 by [adetaylor@google.com](#) on Tue, May 4, 2021, 12:56 PM EDT Project Member

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

Approving merge to M90, branch 4430. Please merge by EOD PST Thursday for inclusion in next week's security refresh.

Comment 22 by [gov...@chromium.org](#) on Tue, May 4, 2021, 2:11 PM EDT Project Member

Please merge your change to M90 branch 4430 ASAP so we can pick it up for next M90 respin. Thank you.

Comment 23 by [Git Watcher](#) on Tue, May 4, 2021, 5:47 PM EDT Project Member

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+4c448c7fa33f21361e816b5fed16ec1e36ec8f5d>

commit [4c448c7fa33f21361e816b5fed16ec1e36ec8f5d](#)

Author: Justin DeWitt <[dewittj@chromium.org](#)>

Date: Tue May 04 21:46:15 2021

Notifications: crash if improper action icons sent from renderer.

Previously, the code only called DCHECK but as this data is from a
renderer we should probably crash the browser.

(cherry picked from commit [3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d](#))

~~Bug-1200040~~

Change-Id: If4d9d48c8e18a3ed9c8bb3a50b952591259e0db5
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2838205>
Commit-Queue: Justin DeWitt <dewittj@chromium.org>
Reviewed-by: Peter Beverloo <peter@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875788}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2872493>
Auto-Submit: Justin DeWitt <dewittj@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Reviewed-by: Adrian Taylor <adetaylor@chromium.org>
Reviewed-by: Krishna Govind <govind@chromium.org>
Owners-Override: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1394}
Cr-Branched-From: [e5ce7dc4f7518237b3d9bb93ccca35d25216cbe](#)-refs/heads/master@{#857950}

[modify] https://crrev.com/4c448c7fa33f21361e816b5fed16ec1e36ec6f5d/chrome/browser/notifications/platform_notification_service_impl.cc
[modify] https://crrev.com/4c448c7fa33f21361e816b5fed16ec1e36ec6f5d/content/browser/notifications/blink_notification_service_impl.cc
[modify] https://crrev.com/4c448c7fa33f21361e816b5fed16ec1e36ec6f5d/content/browser/notifications/blink_notification_service_impl.h

Comment 24 by amyressler@chromium.org on Fri, May 7, 2021, 5:21 PM EDT Project Member
Labels: Release-3-M90

Comment 25 by vsavu@google.com on Mon, May 10, 2021, 9:24 AM EDT Project Member
Labels: LTS-Merge-Request-86 LTS-Security-86

Comment 26 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT Project Member
Labels: CVE-2021-30512 CVE_description-missing

Comment 27 by [Git Watcher](#) on Wed, May 12, 2021, 7:52 AM EDT Project Member
Labels: merge-merged-4430_101

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+df92940ea80e516cc741bfe19ee23b9687ac43b6>

commit [df92940ea80e516cc741bfe19ee23b9687ac43b6](#)
Author: Justin DeWitt <dewittj@chromium.org>
Date: Wed May 12 11:51:09 2021

Notifications: crash if improper action icons sent from renderer.

Previously, the code only called DCHECK but as this data is from a
renderer we should probably crash the browser.

(cherry picked from commit [3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d](#))

(cherry picked from commit [4c448c7fa33f21361e816b5fed16ec1e36ec6f5d](#))

~~Bug-1200040~~

Change-Id: If4d9d48c8e18a3ed9c8bb3a50b952591259e0db5
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2838205>
Commit-Queue: Justin DeWitt <dewittj@chromium.org>
Reviewed-by: Peter Beverloo <peter@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#875788}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2872493>
Auto-Submit: Justin DeWitt <dewittj@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Reviewed-by: Adrian Taylor <adetaylor@chromium.org>
Reviewed-by: Krishna Govind <govind@chromium.org>
Owners-Override: Krishna Govind <govind@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1394}
Cr-Original-Branched-From: [e5ce7dc4f7518237b3d9bb93ccca35d25216cbe](#)-refs/heads/master@{#857950}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2884075>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@{#27}
Cr-Branched-From: [3e9034a21f4b1f6707146b1309e001c3321ab48a](#)-refs/branch-heads/4430@{#1364}
Cr-Branched-From: [e5ce7dc4f7518237b3d9bb93ccca35d25216cbe](#)-refs/heads/master@{#857950}

[modify] https://crrev.com/df92940ea80e516cc741bfe19ee23b9687ac43b6/chrome/browser/notifications/platform_notification_service_impl.cc
[modify] https://crrev.com/df92940ea80e516cc741bfe19ee23b9687ac43b6/content/browser/notifications/blink_notification_service_impl.cc
[modify] https://crrev.com/df92940ea80e516cc741bfe19ee23b9687ac43b6/content/browser/notifications/blink_notification_service_impl.h

Comment 28 by gianluca@google.com on Wed, May 12, 2021, 12:31 PM EDT Project Member
Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 29 by [Git Watcher](#) on Wed, May 12, 2021, 2:09 PM EDT Project Member
Labels: merge-merged-4240

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+fb27b32078021c3ff911d90428e410c7f2efbafb>

commit [fb27b32078021c3ff911d90428e410c7f2efbafb](#)
Author: Justin DeWitt <dewittj@chromium.org>
Date: Wed May 12 18:08:04 2021

Notifications: crash if improper action icons sent from renderer.

Previously, the code only called DCHECK but as this data is from a
renderer we should probably crash the browser.

(cherry picked from commit [3b28dc50187b22e080ad9c1e4e6c4f3b08f3136d](#))

~~Bug-1200040~~

Change-Id: If4d9d48c8e18a3ed9c8bb3a50b952591259e0db5
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2838205>
Commit-Queue: Justin DeWitt <dewittj@chromium.org>
Reviewed-by: Peter Beverloo <peter@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875788}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2883723>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuth@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1635}
Cr-Branched-From: [f297677702651916bbf65e59c0d4bbd4ce57d1ee](https://chromium-review.googlesource.com/c/chromium/src/+297677702651916bbf65e59c0d4bbd4ce57d1ee)-refs/heads/master@{#800218}

[modify] https://crrev.com/27b32078021c3ff911d90428e410c7f2efbafb/chrome/browser/notifications/platform_notification_service_impl.cc
[modify] https://crrev.com/27b32078021c3ff911d90428e410c7f2efbafb/content/browser/notifications/blink_notification_service_impl.cc
[modify] https://crrev.com/27b32078021c3ff911d90428e410c7f2efbafb/content/browser/notifications/blink_notification_service_impl.h

Comment 30 by danakj@chromium.org on Wed, May 12, 2021, 6:38 PM EDT Project Member

It looks like we have a separate list of NotificationActions and icons for those actions. The icons in NotificationResources should move to be inside each NotificationAction to prevent us from having 2 lists with dependent sizes in a mojom.

I wonder if there's some way to prevent dependent lists like this.

Comment 31 by amyressler@google.com on Wed, May 12, 2021, 7:11 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 32 by amyressler@chromium.org on Wed, May 12, 2021, 7:27 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you \$20,000 for this report. Very nice work!

Comment 33 by dcheng@chromium.org on Wed, May 12, 2021, 7:42 PM EDT Project Member

Cc: dcheng@chromium.org

Can we make a followup fix here? The current way the IPC is structured violates the Mojo guidelines. See <https://chromium.googlesource.com/chromium/src/+refs/heads/main/docs/security/mojo.md#use-structured-types> ("avoid parallel arrays of data")

Comment 34 by amyressler@google.com on Mon, May 17, 2021, 2:16 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 35 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 36 by sheriffbot on Thu, Aug 19, 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