

☆ Starred by 5 users

Owner:

CC:

Status:

Components:

Modified:

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:




OS:

Pri:

Type:

Hotlist-Merge-Review
reward-0
Security_Impact-Stable
Security_Severity-Medium
allpublic
CVE_description-submitted
Target-79
M-79
Merge-Rejected-79
Release-0-M80
CVE-2020-6404

rakina@chromium.org

 kraishree@chromium.org
rakina@chromium.org
adetaylor@chromium.org
xiaoc...@chromium.org
 benmason@chromium.org
pbomm...@chromium.org
 yosin@chromium.org
mas...@chromium.org

Fixed (Closed)

Blink>Editing

May 14, 2020

Linux, Android, Windows, Chrome, Mac

1

Bug-Security

Issue 1024256: Crash in blink::FindBuffer::RangeFromBufferIndex with emoji input

Reported by golde...@gmail.com on Wed, Nov 13, 2019, 9:45 AM EST

 Code

VULNERABILITY DETAILS

Please provide a brief explanation of the security issue.

VERSION

Chrome Version: 78.0.3904.97

Operating System: Ubuntu 19.04, MacOS Mojave, Windows10

REPRODUCTION CASE

Please include a demonstration of the security bug, such as an attached HTML or binary file that reproduces the bug when loaded in Chrome. PLEASE make the file as small as possible and remove any content not required to demonstrate the bug, or any personal or confidential information.

Please attach files directly, not in zip or other archive formats, and if you've created a demonstration site please also attach the files needed to reproduce the demonstration locally.

1.Ctr + f

2.attach file of char copy and paste

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: tab

Crash State: crach reportID c82bab681342fe80

Client ID (if relevant):

CREDIT INFORMATION

Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?

Reporter credit: kanchi

chromeCrash.txt

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

Comment 1 by dominickn@chromium.org on Wed, Nov 13, 2019, 12:46 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: rakina@chromium.org

Cc: xiaoc...@chromium.org yosin@chromium.org

Labels: Security_Impact-Stable Security_Severity-Medium OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1

Components: Blink>Editing

Thanks for the bug report. I can verify this reproduces by pasting the single emoji character in the attachment into the Find box, even on the new tab page.

Crash link: crash/c82bab681342fe80

rakina, the crash link indicates the crash is in blink::FindBuffer::RangeFromBufferIndex
(https://cs.chromium.org/chromium/src/third_party/blink/renderer/core/editing/finder/find_buffer.cc?q=find_buffer.cc&sq=package:chromium&dr&=376)

[Comment 2](#) by [dominickn@chromium.org](#) on Wed, Nov 13, 2019, 5:14 PM EST Project Member
Summary: Crash in blink::FindBuffer::RangeFromBufferIndex with emoji input (was: Security: search of crasherror)

[Comment 3](#) by [rakina@chromium.org](#) on Wed, Nov 13, 2019, 6:38 PM EST Project Member
This is using the same character (Object Replacement Character) as [crbug.com/1020105](#) so merging.

[Comment 4](#) by [rakina@chromium.org](#) on Wed, Nov 13, 2019, 6:38 PM EST Project Member
Status: Duplicate (was: Assigned)
Merged into: 1020105

[Comment 5](#) by [golde...@gmail.com](#) on Wed, Nov 13, 2019, 6:53 PM EST
How can I see it URL?
im permission denied ;,-{

[Comment 6](#) by [rakina@chromium.org](#) on Wed, Nov 13, 2019, 7:04 PM EST Project Member
Status: Assigned (was: Duplicate)
Oh wait no nevermind that might be a different bug. Anyways, I think I know why this might be a problem. We replace unfindable DOM (img, videos, etc) with the object replacement character so actually searching for the object replacement character might break some stuff.

[Comment 7](#) by [golde...@gmail.com](#) on Wed, Nov 13, 2019, 7:22 PM EST
Ok im a wait.
Looking forward to being fixed :-)

[Comment 8](#) by [sheriffbot@chromium.org](#) on Thu, Nov 14, 2019, 9:47 AM EST Project Member
Labels: Target-79 M-79
Setting milestone and target because of Security_Impact=Stable and medium severity.
For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

[Comment 9](#) by [bugdroid](#) on Wed, Nov 20, 2019, 1:33 AM EST Project Member
The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+bcc01c0c6c4a16226262444d78461144fe54a42a>

commit [bcc01c0c6c4a16226262444d78461144fe54a42a](#)
Author: Rakina Zata Amni <[rakina@chromium.org](#)>
Date: Wed Nov 20 06:32:38 2019

Use unicode max codepoint for delimiter instead of ORC, and skip buffers with null NGOffsetMapping

It's possible to try to find the Object Replacement Character (ORC), so we should not use that as a delimiter of invalid elements as we might wrongfully think that the delimiters are an actual match, causing crashes.

Additionally in some cases layout might fail causing the FindBuffer to have null NGOffsetMapping, causing crashes. In this case we should skip the entire block as we can't get the ranges correctly.

Bug: 1020105, 1002753, [4094266](#)
Change-Id: I4c4cc886a84a919a617789db6d3bb0351a5d7477
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1924031>
Reviewed-by: Yoshifumi Inoue <[yosin@chromium.org](#)>
Commit-Queue: Rakina Zata Amni <[rakina@chromium.org](#)>
Cr-Commit-Position: refs/heads/master@{#716882}

[modify] https://crrev.com/bcc01c0c6c4a16226262444d78461144fe54a42a/third_party/blink/renderer/core/editing/finder/find_buffer.cc
[modify] https://crrev.com/bcc01c0c6c4a16226262444d78461144fe54a42a/third_party/blink/renderer/core/editing/finder/find_buffer_test.cc

[Comment 10](#) by [rakina@chromium.org](#) on Wed, Nov 20, 2019, 2:17 AM EST Project Member
Status: Fixed (was: Assigned)

[Comment 11](#) by [sheriffbot@chromium.org](#) on Wed, Nov 20, 2019, 10:45 AM EST Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

[Comment 12](#) by [natashapabrai@google.com](#) on Mon, Dec 2, 2019, 1:08 PM EST Project Member
Labels: reward-topanel

[Comment 13](#) by [sheriffbot@chromium.org](#) on Tue, Dec 3, 2019, 11:11 AM EST Project Member
Labels: Merge-Request-79

Requesting merge to beta M79 because latest trunk commit (716882) appears to be after beta branch point (706915).

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

[Comment 14](#) by [sheriffbot@chromium.org](#) on Tue, Dec 3, 2019, 11:12 AM EST Project Member
Labels: -Merge-Request-79 Hotlist-Merge-Review Merge-Review-79

This bug requires manual review: We are only 6 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://goto.google.com/chrome-release-branch-merge-guidelines>
- 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), [kariahda@](#)(iOS), [cindyb@](#)(ChromeOS), [govind@](#)(Desktop)

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

Comment 15 by [adetaylor@google.com](#) on Tue, Dec 3, 2019, 12:46 PM EST Project Member

Security TPM: we should merge this to M79 if it's deemed to be low stability risk. If there are any concerns it can wait till M80.

Comment 16 by [gov...@chromium.org](#) on Tue, Dec 3, 2019, 12:50 PM EST Project Member

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

Labels: OS-Android

[rakina@yosin@](#), how confident are you on this merge to M79 (if approved) this late in release cycle?

Note: We're cutting M79 Stable RC today.

Comment 17 by [gov...@chromium.org](#) on Tue, Dec 3, 2019, 12:56 PM EST Project Member

Labels: -Merge-Review-79 Merge-Rejected-79

Rejecting merge to M79 per chat with [adetaylor@](#).

Comment 18 by [natashapabrai@google.com](#) on Thu, Dec 5, 2019, 9:38 AM EST Project Member

Labels: -reward-topanel reward-0

Unfortunately the Panel decline to reward this report

Comment 19 by [rakina@chromium.org](#) on Wed, Jan 8, 2020, 6:41 AM EST Project Member

Cc: [krajshree@chromium.org](#) [rakina@chromium.org](#)

[Issue-1030831](#) has been merged into this issue.

Comment 20 by [rakina@chromium.org](#) on Mon, Jan 27, 2020, 7:59 PM EST Project Member

[Issue-1045900](#) has been merged into this issue.

Comment 21 by [adetaylor@google.com](#) on Sat, Feb 1, 2020, 8:13 PM EST Project Member

Labels: Release-0-M80

Comment 22 by [adetaylor@chromium.org](#) on Mon, Feb 3, 2020, 6:48 PM EST Project Member

Labels: CVE-2020-6404 CVE_description-missing

Comment 23 by [dtapu...@chromium.org](#) on Mon, Feb 10, 2020, 11:45 AM EST Project Member

[Issue-1050587](#) has been merged into this issue.

Comment 24 by [adetaylor@chromium.org](#) on Mon, Feb 10, 2020, 4:37 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 25 by [sheriffbot](#) on Wed, Feb 26, 2020, 1:56 PM EST 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 26 by [cemka...@gmail.com](#) on Sun, Mar 15, 2020, 3:31 PM EDT

Greetings,

I also found this bug before. Psa.poc.html demonstrates that this bug can be triggered remotely. As I see the description is as following: "Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to potentially exploit heap corruption via crafted clipboard content".

Maybe this poc can change description and CVSS score as well.

Kind regards,
Cem

poc.html
213 bytes [View](#) [Download](#)

Comment 27 by [adetaylor@chromium.org](#) on Mon, Mar 30, 2020, 12:09 AM EDT Project Member

Thanks, I updated the CVE description a few days ago. Hopefully this has propagated through now.

Comment 28 by [natashapabrai@google.com](#) on Mon, Mar 30, 2020, 11:08 AM EDT Project Member

Labels: -reward-0 reward-topanel

Comment 29 by [natashapabrai@google.com](#) on Wed, Apr 1, 2020, 6:19 PM EDT Project Member

Labels: -reward-topanel reward-0

This report was previously found internally and therefore is not eligible for reward.

Comment 30 by [bugdroid](#) on Thu, May 14, 2020, 2:54 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/tools/build/+ccdc5a961c2791b123753737f05cb1b6d6bfd787>

commit [ccdc5a961c2791b123753737f05cb1b6d6bfd787](#)

Author: Wenbin Zhang <[wenbinzhang@google.com](#)>

Date: Thu May 14 18:53:24 2020

[benchmarking] Processor config uses platform from the tester

Base on the discussion on [a^{bug}.com/1078030](#), we will try to avoid adding new bot type for the new processor VMs, and not to skip the config checks between triggerer and triggerree. This CL will revert the changes from [c^{rev}.com/c/2183230](#) on builder tests, and use 'android' as the platform when creating config for android-pixel2-processor-perf-fyi.

[Bug-chromium-1024266](#)
[Bug-chromium-1078030](#)

Change-Id: [I03b8e95f4ad3be0e31c011534bbad9f200733fd](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/tools/build/+2197774>

Reviewed-by: John Chen <[johnchen@chromium.org](#)>

Reviewed-by: Aaron Gable <agable@chromium.org>
Commit-Queue: Wenbin Zhang <wenbinzhang@google.com>

[modify] https://crrev.com/cdc5a961c2791b123753737f05cb1b6d6bfd787/scripts/slave/README_recipes.md
[modify] https://crrev.com/cdc5a961c2791b123753737f05cb1b6d6bfd787/scripts/slave/recipe_modules/chromium_tests/builders/chromium_perf_fyi.py
[modify] https://crrev.com/cdc5a961c2791b123753737f05cb1b6d6bfd787/scripts/slave/recipe_modules/chromium_tests/tests/builders.py