bugs chromium New issue Open issues Search chromium issue Sign in

☆ Starred by 3 users

Owner:	battre@chromium.org
CC:	adetaylor@chromium.org sko@google.com jarhar@chromium.org adetaylor@google.com schwering@google.com koerber@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Lacros
Pri:	1
Type:	Bug-Security

Security_Severity-Medium
reward-4000
allpublic
reward-inprocess
CVE_description-submitted
Target-95
external_security_report
M-96
Target-96
FoundIn-94
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
merge-merged-4692
merge-merged-97
merge-merged-4758
merge-merged-98
Release-0-M97
CVE-2022-0109

Issue 1261689: Security: scrollTop of ListBox autofill preview discloses sensitive information

Reported by y@ylem.kim on Tue, Oct 19, 2021, 10:20 PM EDT

Code

VULNERABILITY DETAILS

When previewing the suggested value of autofill in ListBox (<select> with size > 2), it is scrolled to the suggested value: https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/core/html/forms/select_type.cc;l=983;drc=5cc43d26e76ee462b6224ec447cef2bc5a41a25e

This can be used to infer the previewed option, disclosing sensitive information:
select.options[Math.round(select.scrollTop * select.options.length / select.scrollHeight) + 1]

* Proposed fix: scrollTop should return 0 if the autofill is being previewed

VERSION

Reproducible on:
- 94.0.4606.61 stable, Windows 10 Version 21H1 (Build 19043.1288)
- 97.0.4674.2 canary, Windows 10 Version 21H1 (Build 19043.1288)
- 94.0.4606.61 stable, Linux 5.11.0-34-generic #40~20.04.1-Ubuntu SMP

REPRODUCTION CASE

1. Add at least one credit card entry in chrome://settings/payments and/or one address entry in chrome://settings/addresses
2. Serve the attached poc.html over a secure origin and navigate to the page (an online version is available in https://me94bk1usdv8c8tfybvy.netlify.app/xyo0vvbwwizlnbpwjp15.html)
3. Click on any input and hover the mouse over an autofill entry OR press the up or down arrow key on focused input to preview autofill.
4. The inferred content will appear below.

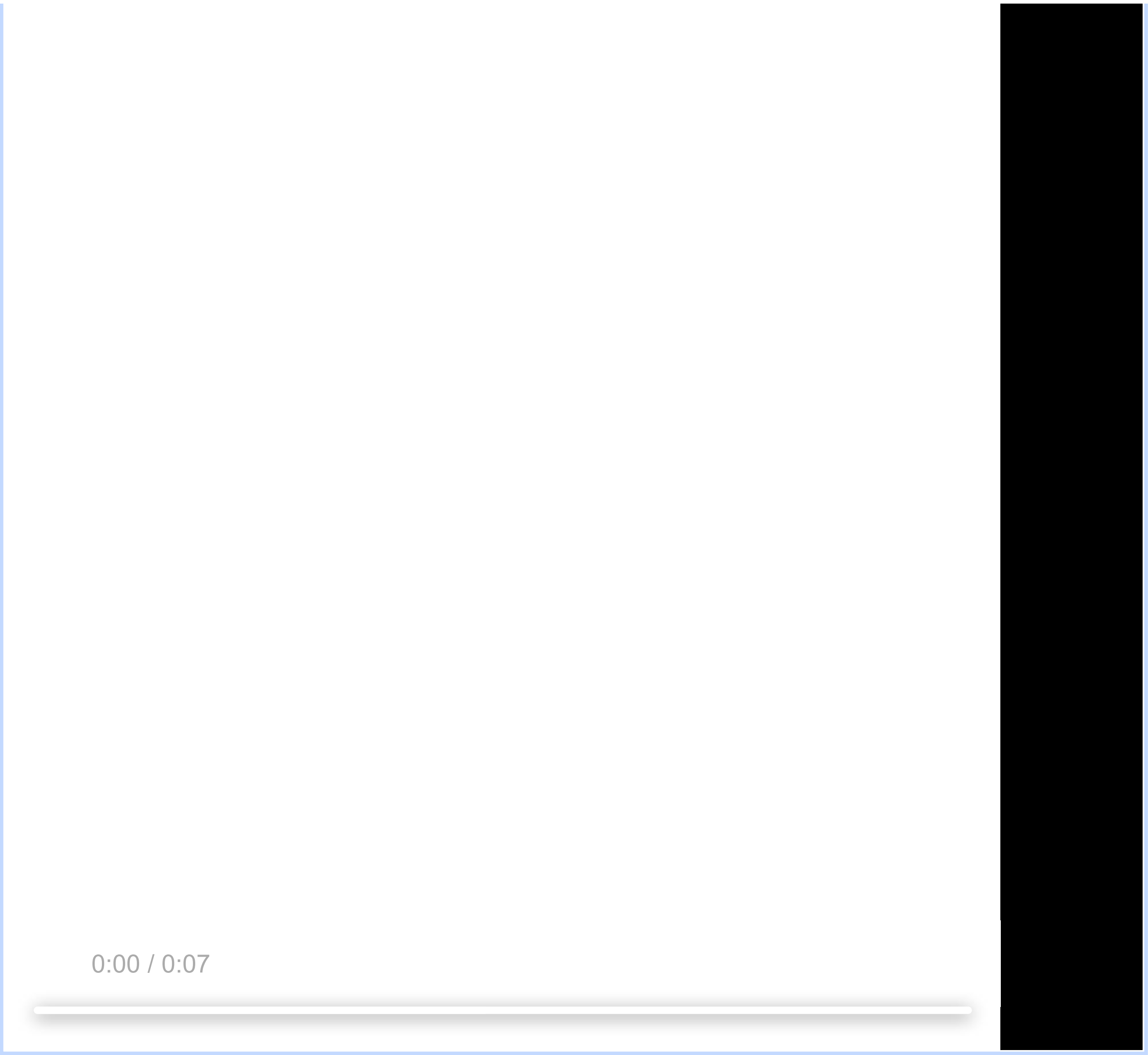
CREDIT INFORMATION

Reporter credit: Young Min Kim (@ylemkimon), CompSec Lab at Seoul National University

poc.html
4.0 KB View Download

poc.mp4
228 KB View Download

[redacted]



Comment 1 by sheriffbot on Tue, Oct 19, 2021, 10:21 PM EDT Project Member

Labels: external_security_report

Comment 2 by y@ylem.kim on Tue, Oct 19, 2021, 10:22 PM EDT

Furthermore, the scroll should be reset if the preview is finished.

Comment 3 by y@ylem.kim on Tue, Oct 19, 2021, 11:29 PM EDT

Real-world scenarios and related bugs are identical to sections 4 and 5 in the ~~issue 1253101~~, respectively.

Please find attached a suggested patch

issue-1261689.patch
1.8 KB View Download

Comment 4 by est...@chromium.org on Wed, Oct 20, 2021, 12:45 AM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: battre@chromium.org
Labels: Security_Severity-Medium FoundIn-94 OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2
Components: UI>Browser>Autofill

Thanks for the report and the patch! Autofill owners, can you please take a look?

Comment 5 by sheriffbot on Wed, Oct 20, 2021, 12:47 AM EDT Project Member

Labels: Security_Impact-Extended

Comment 6 by battre@chromium.org on Wed, Oct 20, 2021, 2:11 AM EDT Project Member

Cc: koerber@google.com schwering@google.com sko@google.com

Thank you for the report and the patch!

Comment 7 by battre@chromium.org on Wed, Oct 20, 2021, 2:21 AM EDT Project Member

Could you explain to me why you made the changes to ListBoxSelectType::DidSetSuggestedOption in your patch?

Comment 8 by y@ylem.kim on Wed, Oct 20, 2021, 2:34 AM EDT

See c#2. The scroll remains after the preview is finished but not applied (selected), so it should be reset to prevent leak. I've chosen `FirstSelectableOption()` because it's available, but it could be scrolled to the top, the first option, or previous saved location.

Comment 9 by sheriffbot on Wed, Oct 20, 2021, 12:52 PM EDT Project Member

Labels: Target-95 M-95

Setting milestone and target because of medium severity.

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

Comment 10 by sheriffbot on Wed, Oct 20, 2021, 1:17 PM EDT Project Member

Labels: -Pri-2 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 11 by sheriffbot on Thu, Nov 4, 2021, 12:21 PM EDT Project Member

battre: Uh oh! This issue still open and hasn't been updated in the last 15 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 12 by sheriffbot on Mon, Nov 15, 2021, 12:21 PM EST Project Member

Labels: -M-95 Target-96 M-96

Comment 13 by Git Watcher on Mon, Nov 15, 2021, 3:59 PM EST Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/55b07dc54220200313366ec821d2303cd847187a

commit 55b07dc54220200313366ec821d2303cd847187a
Author: Dominic Battre <battre@chromium.org>
Date: Mon Nov 15 20:58:16 2021

Pin scrollTop to 0 during autofill preview

This CL forces scrollTop of a ListBox to be 0 during autofill preview
state. After autofill preview ends, it attempts to scroll the ListBox
back so that a previously selected element becomes visible.

~~Fixed: 1261689~~
Change-Id: I8593544577cf054cca40e7a487d3248acdcfdaa7
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3279960
Commit-Queue: Dominic Battré <battre@chromium.org>
Reviewed-by: Mason Freed <masonf@chromium.org>
Cr-Commit-Position: refs/heads/main@{#941822}

[modify]
https://crrev.com/55b07dc54220200313366ec821d2303cd847187a/third_party/blink/renderer/core/html/forms/select_type.cc
[modify]
https://crrev.com/55b07dc54220200313366ec821d2303cd847187a/third_party/blink/web_tests/fast/forms/text/input-appearance-autocomplete-suggested-value-over-placeholder-value-expected.html
[modify]
https://crrev.com/55b07dc54220200313366ec821d2303cd847187a/third_party/blink/renderer/core/testing/internals.cc
[modify]
https://crrev.com/55b07dc54220200313366ec821d2303cd847187a/third_party/blink/web_tests/fast/forms/text/input-appearance-autocomplete-suggested-value-when-underlying-placeholder-is-removed-expected.html
[modify] https://crrev.com/55b07dc54220200313366ec821d2303cd847187a/third_party/blink/renderer/core/dom/element.cc

Comment 14 by sheriffbot on Tue, Nov 16, 2021, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 15 by sheriffbot on Tue, Nov 16, 2021, 1:43 PM EST Project Member

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

Comment 16 by y@ylem.kim on Mon, Nov 22, 2021, 1:47 PM EST

I wonder why the Sheriffbot is not requesting merges, even if this is Medium severity.

Comment 17 by battre@chromium.org on Tue, Nov 23, 2021, 3:38 AM EST Project Member

Cc: adetaylor@chromium.org

+adetaylor regarding comment 16. Shall we merge?

Comment 18 by amyressler@chromium.org on Tue, Nov 23, 2021, 1:40 PM EST Project Member

this is a known issue 1262390; a potential fix has been landed so this shouldn't be an issue soon

Comment 19 by amyressler@chromium.org on Tue, Nov 23, 2021, 1:45 PM EST Project Member

Cc: -adetaylor@chromium.org
Labels: Merge-Review-96 Merge-Review-97

removing ade from cc so he doesn't get pinged on merge review updates; I've added merge review labels so this will add to my review queue - thanks

Comment 20 by amyressler@google.com on Tue, Nov 23, 2021, 7:21 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-4000

*** 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 21 by amyressler@chromium.org on Tue, Nov 23, 2021, 8:07 PM EST Project Member

Congratulations! The VRP Panel has decided to award you $4000 for this report. A member of our finance team will be in touch soon to arrange payment. Thank you for your report and nice work!!

Comment 22 by amyressler@google.com on Wed, Nov 24, 2021, 2:56 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 23 by y@ylem.kim on Fri, Nov 26, 2021, 8:39 PM EST

It turns out that pinning scrollTop to 0 when the suggested value is empty also leaks the suggested option, as the suggested value becomes empty when the suggested option is removed (https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/core/html/forms/html_select_element.cc;l=784-785;drc=66f8666257dd5d2687c37c155f40cc72e0176270). Instead, it should check for the autofill state, which doesn't change even after the suggested option is removed. Please find attached the new PoC and patch. The reproduction steps are identical, and the online version is available in https://me94bk1usdv8c8tfybvy.netlify.app/xyo0vvbwwizlnbpwjp15-2.html.

poc-2.html
4.2 KB View Download

issue-1261689-2.patch
1.2 KB View Download

Comment 24 by amyressler@chromium.org on Mon, Nov 29, 2021, 2:29 PM EST Project Member

Status: Started (was: Fixed)

I've re-opened this based on the new POC in comment #23 and verifying this does indeed reproduce with the new POC. battre@ would you mind taking a look at this?

Comment 25 by amyressler@chromium.org on Mon, Nov 29, 2021, 2:31 PM EST Project Member

based on the above, going to not approve merge of the earlier landed fix for now until this is reassessed

Comment 26 by adetaylor@google.com on Mon, Dec 13, 2021, 12:47 PM EST Project Member

Cc: adetaylor@chromium.org

Comment 27 by battre@chromium.org on Mon, Dec 13, 2021, 4:50 PM EST Project Member

Thanks for the reminder, Adrian. I have submitted a CL for review here: https://chromium-review.googlesource.com/c/chromium/src/+/3335637

Thank you for the followup and patch.

I would prefer to merge both CLs together.

Comment 28 by adetaylor@chromium.org on Mon, Dec 13, 2021, 6:44 PM EST Project Member

Great. Thank you for following up. When that follow up CL lands, please mark this as Fixed and it will go into the queue for merge approval.

Comment 29 by Git Watcher on Mon, Dec 13, 2021, 9:08 PM EST Project Member

Status: Fixed (was: Started)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e3aeadcf584ebb5d7f61cd141f9af317cb60cf21

commit e3aeadcf584ebb5d7f61cd141f9af317cb60cf21
Author: Dominic Battre <battre@chromium.org>
Date: Tue Dec 14 02:07:29 2021

Fix preview state detection

This CL fixes the preview state detection in some edge cases. See
~~crbug.com/1261689#c23~~.

~~Fixed: 1261689~~
Change-Id: Iefe27e2748acb4b524e8a0811973bdceda46089a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3335637
Reviewed-by: Mason Freed <masonf@chromium.org>
Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Commit-Position: refs/heads/main@{#951313}

[modify] https://crrev.com/e3aeadcf584ebb5d7f61cd141f9af317cb60cf21/third_party/blink/renderer/core/dom/element.cc

Comment 30 by adetaylor@google.com on Wed, Dec 15, 2021, 12:04 PM EST Project Member

Labels: -Merge-Review-96 -Merge-Review-97 Merge-Approved-97 Self-Merge-Approved-97 Merge-Approved-98

Approving merge to M96, branch 4664, and M97, branch 4692, but please wait until the CL in #c29 has had 48 hours in Canary and confirm that there are no unexpected crashes from the relevant code. We're not imminently about to cut a release RC so it's OK if this doesn't land in those branches for a couple of days, but it would be great to get it in before the release RC so it's OK if this doesn't land in those branches for a couple of days, but it would be great to get it in before the holiday break on the assumption that we might make a release immediately after the holidays (no such release is planned, but it would be surprising if no events necessitated it!)

Also approving merge of #c29 to M98, branch 4758, because it landed after M98 branch point.

Comment 31 by adetaylor@google.com on Wed, Dec 15, 2021, 12:05 PM EST Project Member

Labels: -Self-Merge-Approved-97 Merge-Approved-96

Comment 32 by battre@chromium.org on Mon, Dec 20, 2021, 3:26 AM EST Project Member

Cc: jarhar@chromium.org

Adding jarhar@ because I will request a merge review.

Comment 33 by Git Watcher on Mon, Dec 20, 2021, 11:42 AM EST Project Member

Labels: -merge-approved-97 merge-merged-4692 merge-merged-97

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/9817ab616338df9cf1dbbbec6e589c4abfcacffb

commit 9817ab616338df9cf1dbbbec6e589c4abfcacffb
Author: Dominic Battre <battre@chromium.org>
Date: Mon Dec 20 16:41:52 2021

Pin scrollTop to 0 during autofill preview

This CL forces scrollTop of a ListBox to be 0 during autofill preview
state. After autofill preview ends, it attempts to scroll the ListBox
back so that a previously selected element becomes visible.

(cherry picked from commit 55b07dc54220200313366ec821d2303cd847187a)

~~Fixed: 1261689~~
Change-Id: I8593544577cf054cca40e7a487d3248acdcfdaa7
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3279960
Commit-Queue: Dominic Battré <battre@chromium.org>
Reviewed-by: Mason Freed <masonf@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#941822}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347569
Auto-Submit: Dominic Battré <battre@chromium.org>
Reviewed-by: Joey Arhar <jarhar@chromium.org>
Commit-Queue: Joey Arhar <jarhar@chromium.org>
Cr-Commit-Position: refs/branch-heads/4692@{#1097}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify]
https://crrev.com/9817ab616338df9cf1dbbbec6e589c4abfcacffb/third_party/blink/renderer/core/html/forms/select_type.cc
[modify] https://crrev.com/9817ab616338df9cf1dbbbec6e589c4abfcacffb/third_party/blink/web_tests/fast/forms/text/input-appearance-autocomplete-suggested-value-over-placeholder-value-expected.html
[modify] https://crrev.com/9817ab616338df9cf1dbbbec6e589c4abfcacffb/third_party/blink/renderer/core/testing/internals.cc

[modify] https://crrev.com/9817ab616338df9cf1dbbbec6e589c4abfcacffb/third_party/blink/web_tests/fast/forms/text/input-appearance-autocomplete-suggested-value-when-underlying-placeholder-is-removed-expected.html
[modify] https://crrev.com/9817ab616338df9cf1dbbbec6e589c4abfcacffb/third_party/blink/renderer/core/dom/element.cc

[modify] https://crrev.com/9817ab616338df9cf1dbbbec6e589c4abfcacfb/third_party/blink/renderer/core/dom/element.cc

Comment 34 by sheriffbot on Mon, Dec 20, 2021, 12:20 PM EST Project Member

Cc: adetaylor@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 35 by Git Watcher on Mon, Dec 20, 2021, 1:54 PM EST Project Member

Labels: -merge-approved-96 merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/cff03c22c54b3bbdb0642b9062855f5f77f9d12a

commit cff03c22c54b3bbdb0642b9062855f5f77f9d12a
Author: Dominic Battre <battre@chromium.org>
Date: Mon Dec 20 18:53:00 2021

Pin scrollTop to 0 during autofill preview

This CL forces scrollTop of a ListBox to be 0 during autofill preview
state. After autofill preview ends, it attempts to scroll the ListBox
back so that a previously selected element becomes visible.

(cherry picked from commit 55b07dc54220200313366ec821d2303cd847187a)

~~Fixed: 1261689~~
Change-Id: I8593544577cf054cca40e7a487d3248acdcfdaa7
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3279960
Commit-Queue: Dominic Battré <battre@chromium.org>
Reviewed-by: Mason Freed <masonf@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#941822}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347570
Auto-Submit: Dominic Battré <battre@chromium.org>
Reviewed-by: Joey Arhar <jarhar@chromium.org>
Commit-Queue: Joey Arhar <jarhar@chromium.org>
Cr-Commit-Position: refs/branch-heads/4664@{#1330}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/cff03c22c54b3bbdb0642b9062855f5f77f9d12a/third_party/blink/renderer/core/html/forms/select_type.cc
[modify] https://crrev.com/cff03c22c54b3bbdb0642b9062855f5f77f9d12a/third_party/blink/web_tests/fast/forms/text/input-appearance-autocomplete-suggested-value-over-placeholder-value-expected.html
[modify] https://crrev.com/cff03c22c54b3bbdb0642b9062855f5f77f9d12a/third_party/blink/renderer/core/testing/internals.cc
[modify] https://crrev.com/cff03c22c54b3bbdb0642b9062855f5f77f9d12a/third_party/blink/web_tests/fast/forms/text/input-appearance-autocomplete-suggested-value-when-underlying-placeholder-is-removed-expected.html
[modify] https://crrev.com/cff03c22c54b3bbdb0642b9062855f5f77f9d12a/third_party/blink/renderer/core/dom/element.cc

Comment 36 by Git Watcher on Mon, Dec 20, 2021, 5:38 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/76ee5ef9198eeb8185bfa6a90b12495ae891c563

commit 76ee5ef9198eeb8185bfa6a90b12495ae891c563
Author: Dominic Battre <battre@chromium.org>
Date: Mon Dec 20 22:37:51 2021

Fix preview state detection

This CL fixes the preview state detection in some edge cases. See
~~crbug.com/1261689#c23~~.

(cherry picked from commit e3aeadcf584ebb5d7f61cd141f9af317cb60cf21)

~~Fixed: 1261689~~
Change-Id: Iefe27e2748acb4b524e8a0811973bdceda46089a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3335637
Reviewed-by: Mason Freed <masonf@chromium.org>
Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#951313}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3350770
Auto-Submit: Dominic Battré <battre@chromium.org>
Reviewed-by: Joey Arhar <jarhar@chromium.org>
Commit-Queue: Joey Arhar <jarhar@chromium.org>
Cr-Commit-Position: refs/branch-heads/4664@{#1332}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/76ee5ef9198eeb8185bfa6a90b12495ae891c563/third_party/blink/renderer/core/dom/element.cc

Comment 37 by Git Watcher on Tue, Dec 21, 2021, 1:02 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/896620bfe9d405cde104d74347e300d1ddb03c21

commit 896620bfe9d405cde104d74347e300d1ddb03c21
Author: Dominic Battre <battre@chromium.org>
Date: Tue Dec 21 18:01:14 2021

Fix preview state detection

This CL fixes the preview state detection in some edge cases. See
~~crbug.com/1261689#c23~~.

(cherry picked from commit e3aeadcf584ebb5d7f61cd141f9af317cb60cf21)

~~Fixed: 1261689~~
Change-Id: Iefe27e2748acb4b524e8a0811973bdceda46089a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3335637
Reviewed-by: Mason Freed <masonf@chromium.org>

Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#951313}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3350768

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3350768
Auto-Submit: Dominic Battré <battre@chromium.org>
Reviewed-by: Joey Arhar <jarhar@chromium.org>
Cr-Commit-Position: refs/branch-heads/4692@{#1117}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify] https://crrev.com/896620bfe9d405cde104d74347e300d1ddb03c21/third_party/blink/renderer/core/dom/element.cc

Comment 38 by battre@chromium.org on Wed, Dec 22, 2021, 4:08 AM EST Project Member

All merging should be done.

Comment 39 by y@ylem.kim on Wed, Dec 22, 2021, 4:20 AM EST

Sorry for chiming in, but it seems it's not merged to M98 (4758). Thank you for your hard work.

Comment 40 by battre@chromium.org on Wed, Dec 22, 2021, 4:35 AM EST Project Member

Oh... Thanks for catching this! I have created https://chromium-review.googlesource.com/c/chromium/src/+/3348406.

Comment 41 by Git Watcher on Wed, Dec 22, 2021, 11:26 AM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/91fbf179875be529f32f4ad2ba83186f9c072641

commit 91fbf179875be529f32f4ad2ba83186f9c072641
Author: Dominic Battre <battre@chromium.org>
Date: Wed Dec 22 16:25:16 2021

Fix preview state detection

This CL fixes the preview state detection in some edge cases. See
~~crbug.com/1261689#c23~~.

(cherry picked from commit e3aeadcf584ebb5d7f61cd141f9af317cb60cf21)

~~Fixed: 1261689~~
Change-Id: Iefe27e2748acb4b524e8a0811973bdceda46089a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3335637
Reviewed-by: Mason Freed <masonf@chromium.org>
Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#951313}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3348406
Auto-Submit: Dominic Battré <battre@chromium.org>
Reviewed-by: Joey Arhar <jarhar@chromium.org>
Commit-Queue: Joey Arhar <jarhar@chromium.org>
Cr-Commit-Position: refs/branch-heads/4758@{#186}
Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify] https://crrev.com/91fbf179875be529f32f4ad2ba83186f9c072641/third_party/blink/renderer/core/dom/element.cc

Comment 42 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:09 PM EST Project Member

Labels: Release-0-M97

Comment 43 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0109 CVE_description-missing

Comment 44 by sheriffbot on Tue, Mar 22, 2022, 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

Comment 45 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted