☆ Starred by 5 users

Owner:	fhorschig@chromium.org
CC:	adetaylor@chromium.org battre@chromium.org schwering@google.com est...@chromium.org mamir@chromium.org koerber@google.com mlerman@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill
Modified:	Aug 25, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Android
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
LTS-Security-86
LTS-Security-NotApplicable-86
external_security_report
merge-merged-4472
merge-merged-91
LTS-Security-90
LTS-Security-NotApplicable-90
Release-0-M91
CVE-2021-30521

Issue 1208721: Security: heap-over-flow in AutofillPopupControllerImpl::RemoveSuggestion

Reported by zhanj...@gmail.com on Thu, May 13, 2021, 1:19 AM EDT

Code

VULNERABILITY DETAILS

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/autofill/autofill_keyboard_accessory_adapter.cc;l=127;drc=2f8e0536eb97ce2131e7a74e3ca06077aa0b64b3;bpv=1;bpt=1

```
bool AutofillKeyboardAccessoryAdapter::RemoveSuggestion(int index) {
  DCHECK(view_) << "RemoveSuggestion called before a View was set!";
  std::u16string title, body;
  if (!GetRemovalConfirmationText(index, &title, &body))
    return false;

  view_->ConfirmDeletion(
      title, body,
      base::BindOnce(&AutofillKeyboardAccessoryAdapter::OnDeletionConfirmed,             //[1]
                     weak_ptr_factory_.GetWeakPtr(), index));
  return true;
}
```

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/autofill/autofill_keyboard_accessory_adapter.cc;drc=2f8e0536eb97ce2131e7a74e3ca06077aa0b64b3;bpv=1;bpt=1;l=216

```
void AutofillKeyboardAccessoryAdapter::OnDeletionConfirmed(int index) {
  if (controller_)
    controller_->RemoveSuggestion(OffsetIndexFor(index));            //[2]
}
```

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/autofill/autofill_popup_controller_impl.cc;drc=2f8e0536eb97ce2131e7a74e3ca06077aa0b64b3;bpv=1;bpt=1;l=352

```
bool AutofillPopupControllerImpl::RemoveSuggestion(int list_index) {
  if (!delegate_->RemoveSuggestion(suggestions_[list_index].value,          //[3]
                                   suggestions_[list_index].frontend_id)) {
    return false;
  }

  // Remove the deleted element.
  suggestions_.erase(suggestions_.begin() + list_index);        //[4]

  selected_line_.reset();

  if (HasSuggestions()) {
    delegate_->ClearPreviewedForm();
    OnSuggestionsChanged();
  } else {
    Hide(PopupHidingReason::kNoSuggestions);
  }
  return true;
}
```

AutofillKeyboardAccessoryAdapter::OnDeletionConfirmed callback hold an `index`, the `index` is used for accessing `suggestions_`[3][4] when user confirm that.
`suggestions_`'s size can be changed while the confirm dialog is showing, then click the OK button, heap-over-flow occurs.

VERSION
Chrome Version: [Chrome 90.0.4430.210] + [stable]
Operating System: [Android 8.0.0; SM-G965F Build/R16NW]

REPRODUCTION CASE

1. python3 -m http.server
2. visit test.html
3. cache two suggestions "aa" and "bb"
4. click the input control, press a and then hold the second suggestion on the popup, wait a second, click OK button

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: [browser]
Crash State: [see link above: stack trace *with symbols*, registers, exception record]
Client ID (if relevant): [see link above]

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: [goes here]

Comment 1 by sheriffbot on Thu, May 13, 2021, 1:24 AM EDT

Labels: external_security_report

Comment 2 by zhanj...@gmail.com on Thu, May 13, 2021, 1:33 AM EDT

test.html
590 bytes View Download

tombstone_06
637 KB View Download

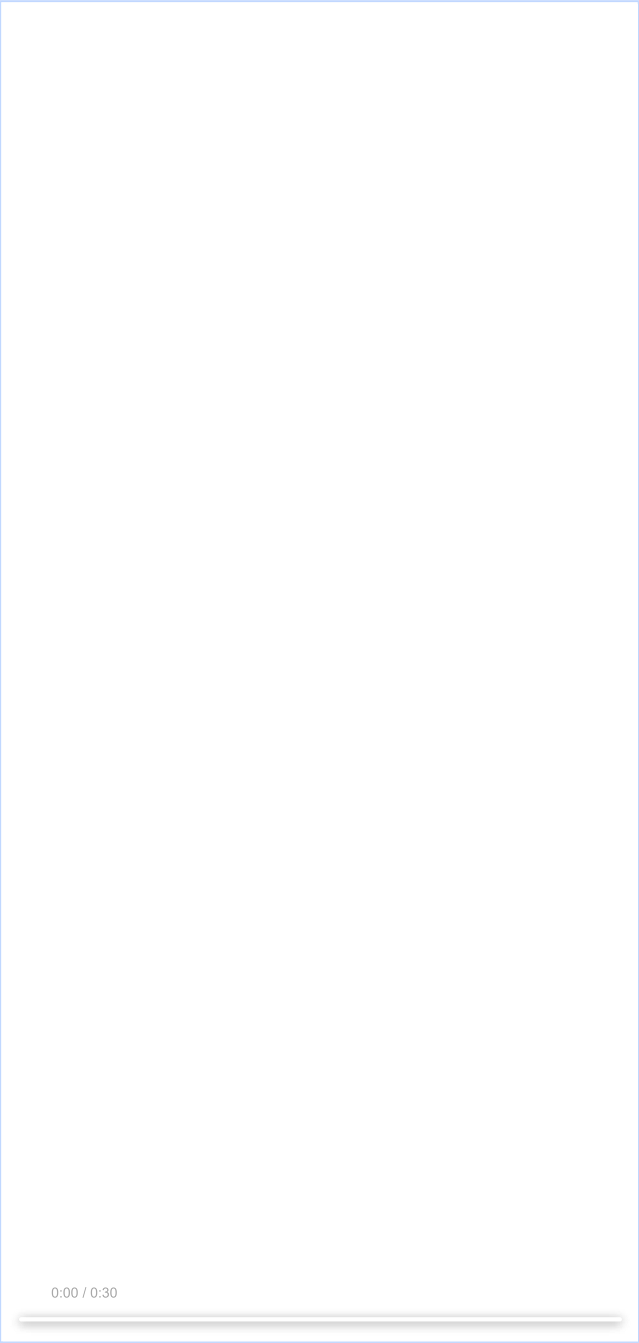
20210513_132138.mp4
7.8 MB View Download

Comment 3 by zhanj...@gmail.com on Thu, May 13, 2021, 2:39 AM EDT
compile chrome_public_apk and test it on arm64 device.

debuginfo.txt
16.7 KB View Download

tombstone_03
1.1 MB View Download

20210513_142803.mp4
11.5 MB View Download



Comment 4 by xinghuilu@chromium.org on Thu, May 13, 2021, 2:57 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: fhorschig@chromium.org
Cc: est...@chromium.org mamir@chromium.org schwering@google.com
Labels: Security_Impact-Stable Security_Severity-High OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Browser>Autofill

Thanks for the report! fhorschig@, could you take a look? Thanks! Assigning high severity due to the interaction required.

Comment 5 by schwering@google.com on Fri, May 14, 2021, 6:38 AM EDT

Cc: battre@chromium.org koerber@google.com

Comment 6 by sheriffbot on Fri, May 14, 2021, 12:47 PM EDT

Labels: M-90 Target-90

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 7 by zhanj...@gmail.com on Fri, May 14, 2021, 9:53 PM EDT

caching suggestions and shrinking `suggestion_`'s size can be done by a compromised renderer, the only interaction required is choosing a suggestion to delete.

Comment 8 by fhorschig@chromium.org on Mon, May 17, 2021, 4:25 AM EDT

Status: Started (was: Assigned)
Labels: -OS-Linux -OS-Windows -OS-Chrome -OS-Mac

Thanks for the detailed reproduction steps!

This is indeed an issue and (as was demonstrated) affects at least all Android surfaces. The accessory path was mentioned in #1 and is seen in #3 and the dropdown path as seen in #2 doesn't use a callback but stores the index until the dialog confirmation returns [1].

The deletion on Desktop platforms use a different path (e.g. on Linux Shift + Del while focusing a item in the dropdown) and therefore don't seem affected (i.e. because the dropdown is updated with further input and there isn't even a confirmation dialog). I haven't checked what iOS does but it doesn't seem to use any of the involved classes.

I'll start a fix that just aborts the removal operation if the index is out of bounds which should be easy to merge to any branch.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/android/autofill/autofill_popup_view_android.cc;l=142;drc=46bbb9795fcc1934c6cfbec096764f888c4d400a

Comment 9 by Git Watcher on Mon, May 17, 2021, 7:18 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/995e7b9aba32b194962d98b0bf44e8fe03d4011e

commit 995e7b9aba32b194962d98b0bf44e8fe03d4011e
Author: Friedrich Horschig <fhorschig@chromium.org>
Date: Mon May 17 11:17:16 2021

[Android] Fix trying to remove out-of-bounds autofill suggestion

If the suggestions known to the popup controller change but a removal
confirmation is still pending, the index held by the confirmation is out
of date and can either:
* delete an incorrect suggestions or
* cause a crash due to an out-of-bounds access.

This CL only fixes the latter case but might need to be merged.
A proper fix would involve wide-spread changes to the identification
of a selected suggestions (see https://crbug.com/1209792).

~~Bug: 1208721~~
Change-Id: Ib5d352b1752583faf01aa28ef61c983f0c655921
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2896977
Commit-Queue: Friedrich [CET] <fhorschig@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Cr-Commit-Position: refs/heads/master@{#883425}

[modify] https://crrev.com/995e7b9aba32b194962d98b0bf44e8fe03d4011e/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 10 by fhorschig@chromium.org on Mon, May 17, 2021, 10:13 AM EDT
Status: Fixed (was: Started)
Cc: adetaylor@chromium.org

@adetaylor: Can you please help us to figure out which milestone this should go into?
(The bug says M90 but M91 is already cut in two days. And although it's an easy fix, I am not sure merging to M91 would still be accepted.)

Comment 11 by sheriffbot on Mon, May 17, 2021, 12:42 PM EDT
Labels: reward-topanel

Comment 12 by sheriffbot on Mon, May 17, 2021, 2:01 PM EDT
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 13 by sheriffbot on Mon, May 17, 2021, 2:21 PM EDT
Labels: Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (883425) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (883425) appears to be after beta branch point (965).

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

Comment 14 by sheriffbot on Mon, May 17, 2021, 2:22 PM EDT
Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: We are only 7 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), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 15 by adetaylor@google.com on Mon, May 17, 2021, 2:59 PM EDT
Labels: -Merge-Review-91 Merge-Approved-91

Approving merge to M91; please merge to branch 4472.

Comment 16 by Git Watcher on Tue, May 18, 2021, 3:58 AM EDT
Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d8cb34212e2383a6b87c2f37060013eb82de1541

commit d8cb34212e2383a6b87c2f37060013eb82de1541
Author: Friedrich Horschig <fhorschig@chromium.org>
Date: Tue May 18 07:57:37 2021

[Android] Fix trying to remove out-of-bounds autofill suggestion

If the suggestions known to the popup controller change but a removal

confirmation is still pending, the index held by the confirmation is out
of date and can either:
* delete an incorrect suggestions or
* cause a crash due to an out-of-bounds access.

This CL only fixes the latter case but might need to be merged.
A proper fix would involve wide-spread changes to the identification
of a selected suggestions (see https://crbug.com/1209792).

(cherry picked from commit 995e7b9aba32b194962d98b0bf44e8fe03d4011e)

~~Bug: 1208721~~
Change-Id: Ib5d352b1752583faf01aa28ef61c983f0c655921
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2896977
Commit-Queue: Friedrich [CET] <fhorschig@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#883425}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2902703
Auto-Submit: Friedrich [CET] <fhorschig@chromium.org>
Commit-Queue: Marc Treib <treib@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#1136}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/d8cb34212e2383a6b87c2f37060013eb82de1541/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 17 by amyressler@google.com on Thu, May 20, 2021, 1:08 PM EDT
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 18 by amyressler@chromium.org on Thu, May 20, 2021, 5:24 PM EDT
Congratulations! The VRP Panel has decided to award you $20,000 for this report. Excellent work!!

Comment 19 by adetaylor@google.com on Fri, May 21, 2021, 3:43 PM EDT
Labels: -Merge-Request-90

Comment 20 by amyressler@google.com on Fri, May 21, 2021, 5:27 PM EDT
Labels: -reward-unpaid reward-inprocess

Comment 21 Deleted

Comment 22 by amyressler@chromium.org on Mon, May 24, 2021, 11:01 AM EDT
Labels: -Release-1-M91 Release-0-M91

Comment 23 by amyressler@google.com on Mon, May 24, 2021, 2:17 PM EDT
Labels: CVE-2021-30521 CVE_description-missing

Comment 24 by amyressler@chromium.org on Mon, May 24, 2021, 2:28 PM EDT
Hello zhanjiasong@- we consider attachments/pocs included with reports to be an integral part of the report, so I've un-deleted them. Thanks!

Comment 25 by achuith@chromium.org on Thu, May 27, 2021, 11:52 AM EDT
Labels: LTS-Security-NotApplicable-86 LTS-Security-86

Comment 26 by asumaneev@google.com on Mon, Jun 7, 2021, 2:54 PM EDT
Labels: LTS-Security-90 LTS-Security-NotApplicable-90

Marking not applicable for LTS since Android-only issue.

Comment 27 by amyressler@google.com on Mon, Jun 7, 2021, 3:26 PM EDT
Labels: -CVE_description-missing CVE_description-submitted

Comment 28 by sheriffbot on Wed, Aug 25, 2021, 1:30 PM EDT
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