Starred by 7 users

Owner:	schwering@google.com
CC:	battre@chromium.org adetaylor@google.com treib@chromium.org schwering@google.com mamir@chromium.org mamir@google.com koerber@google.com mac-bugs-priority@chromium.org mlerman@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill
Modified:	Aug 25, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
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-2021-30514

Issue 1200766: UAF in AutofillPopupControllerImpl

Reported by super...@gmail.com on Tue, Apr 20, 2021, 7:12 AM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36

Steps to reproduce the problem:
1. Type "aaaaaaa" in the form and click 'Submit' button
2. return to poc1.html
3. Type "a" in the form to show the suggestion:"aaaaaa"
4. waiting for the form be large and type "a" to trigger the uaf

steps 1、2 is not needed if the form already have suggestion.

What is the expected behavior?

What went wrong?
AutofillPopupControllerImpl::Show[1] will call AutofillPopupControllerImpl::OnSuggestionsChanged()[2]

And if dropdown can not be shown.AutofillPopupControllerImpl::OnSuggestionsChanged()will call following chain:
AutofillPopupControllerImpl::OnSuggestionsChanged()->
AutofillPopupViewNativeViews::OnSuggestionsChanged()->
AutofillPopupViewNativeViews::DoUpdateBoundsAndRedrawPopup()->
AutofillPopupControllerImpl::Hide() (if !CanShowDropdownHere)->
AutofillPopupControllerImpl::HideViewAndDie() <- delete this

So when OnSuggestionsChanged() return.UAF will be trigger when accessing delegate[3]

```
void AutofillPopupControllerImpl::Show(  ---------- [1]
    const std::vector<Suggestion>& suggestions,
    bool autoselect_first_suggestion,
    PopupType popup_type) {
  SetValues(suggestions);

  bool just_created = false;
  if (!view_) {
    view_ = AutofillPopupView::Create(GetWeakPtr());

    // It is possible to fail to create the popup, in this case
    // treat the popup as hiding right away.
    if (!view_) {
      delegate_->OnPopupSuppressed();
      Hide(PopupHidingReason::kViewDestroyed);
      return;
    }
    just_created = true;
  }
```

```
  if (just_created) {
#if defined(OS_ANDROID)
    ManualFillingController::GetOrCreate(web_contents_)
        ->UpdateSourceAvailability(FillingSource::AUTOFILL,
                                   !suggestions.empty());
#endif
    WeakPtr<AutofillPopupControllerImpl> weak_this = GetWeakPtr();
    view_->Show();
    // crbug.com/1055981. |this| can be destroyed synchronously at this point.
    if (!weak_this)
      return;

    // We only fire the event when a new popup shows. We do not fire the
    // event when suggestions changed.
    FireControlsChangedEvent(true);

    if (autoselect_first_suggestion)
      SetSelectedLine(0);
  } else {
    if (selected_line_ && *selected_line_ >= GetLineCount())
      selected_line_.reset();

    OnSuggestionsChanged(); ----------------------------[2]
  }

  static_cast<ContentAutofillDriver*>(delegate_->GetAutofillDriver())----------------------------[3]
      ->RegisterKeyPressHandler(base::BindRepeating(
          [](base::WeakPtr<AutofillPopupControllerImpl> weak_this,
             const content::NativeWebKeyboardEvent& event) {
            return weak_this && weak_this->HandleKeyPressEvent(event);
          },
          GetWeakPtr()));

  delegate_->OnPopupShown();
}
```

Did this work before? N/A

Chrome version: Channel: n/a
OS Version:
Flash Version:

asan.log
19.1 KB View Download

poc1.html
375 bytes View Download

Comment 1 by sheriffbot on Tue, Apr 20, 2021, 7:17 AM EDT

Labels: external_security_report

Comment 2 by super...@gmail.com on Tue, Apr 20, 2021, 8:27 AM EDT

[Deleted] **a.mp4**

Comment 3 Deleted

Comment 4 by ClusterFuzz on Tue, Apr 20, 2021, 8:27 PM EDT

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=6298525420552192.

Comment 5 by super...@gmail.com on Wed, Apr 21, 2021, 8:24 AM EDT

Hi, I update my poc so that this bug can be trigger just type an "a" in the form.

Steps to reproduce the problem:

1、 php -S 0.0.0.0:8081 (python is not supported "post" so use php)
2、out/asan/Chromium.app/Contents/MacOS/Chromium "http://localhost:8081/poc1.html"
3、 click the form text and type "a" then the browser will be crashed(with asan)

poc1.html
621 bytes View Download

Comment 6 by carlosil@chromium.org on Wed, Apr 21, 2021, 9:43 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: est...@chromium.org
Labels: Security_Impact-Stable Security_Severity-High
Components: UI>Browser>Autofill

Looks like clusterfuzz couldn't reproduce due to the required interaction, but this seems otherwise like a legitimate bug. Assigning high severity due to the interaction required

estade: Passing to you as an owner of the relevant code, please reassign as appropriate. Thanks!

Comment 7 by est...@chromium.org on Thu, Apr 22, 2021, 12:03 AM EDT

Owner: battre@chromium.org

Comment 8 by super...@gmail.com on Thu, Apr 22, 2021, 1:50 AM EDT

The following 1.mp4 show the #c5 steps to reproduce the problem without a compromised renderer.It just need simple and normal user interaction.

And since ShowSuggestions is a mojom interface.I think the bug can be triggered without user interaction by a compromised renderer.

1.mp4
649 KB View Download

Comment 9 by battre@chromium.org on Thu, Apr 22, 2021, 7:27 AM EDT

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

Comment 10 by koerber@google.com on Thu, Apr 22, 2021, 7:29 AM EDT

Cc: mamir@google.com

Comment 11 by mamir@chromium.org on Thu, Apr 22, 2021, 10:38 AM EDT

Owner: mamir@chromium.org

Comment 12 by mamir@chromium.org on Thu, Apr 22, 2021, 10:42 AM EDT

Cc: koerber@google.com

Comment 13 by mamir@chromium.org on Thu, Apr 22, 2021, 11:40 AM EDT

Status: Started (was: Assigned)
Owner: schwering@google.com

Christoph most of the work, so it makes he owns it.

Comment 14 by mamir@chromium.org on Thu, Apr 22, 2021, 11:59 AM EDT

Cc: treib@chromium.org

Comment 15 by Git Watcher on Thu, Apr 22, 2021, 12:43 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ce5bb101c32b4e007c339aea3f9d57b91ed29e47

commit ce5bb101c32b4e007c339aea3f9d57b91ed29e47
Author: Christoph Schwering <schwering@google.com>
Date: Thu Apr 22 16:42:45 2021

[Autofill] Fixed disappearing Autofill popup.

~~Bug: 1200766~~
Change-Id: I72a582326c183e0cc9ad226d95cae6d118a0b7a2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2846511
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Commit-Position: refs/heads/master@{#875206}

[modify] https://crrev.com/ce5bb101c32b4e007c339aea3f9d57b91ed29e47/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 16 by sheriffbot on Thu, Apr 22, 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 17 by sheriffbot on Thu, Apr 22, 2021, 1:27 PM EDT

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity High. 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 18 Deleted

Comment 19 by schwering@google.com on Mon, Apr 26, 2021, 12:52 PM EDT

Cc: adetaylor@google.com
Labels: Merge-Request-91

Firstly, thanks for reporting!

The CL from comment 15 fixes the UAF.

Requesting merge for M91, will request M90 once it's been on Dev.

Comment 20 by sheriffbot on Mon, Apr 26, 2021, 12:57 PM EDT

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), bindusuvarna@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 21 by schwering@google.com on Mon, Apr 26, 2021, 1:02 PM EDT

1. Yes, it's a security bug and the fix has a low complexity.
2. https://chromium-review.googlesource.com/c/chromium/src/+/2846511
3. Yes.
4. I suppose so.
5. Security bug.
6. No.
7. N/A.

Comment 22 by adetaylor@google.com on Mon, Apr 26, 2021, 1:04 PM EDT

Labels: -Merge-Review-91 Merge-Approved-91 Merge-Request-90

Please mark it as Fixed if it is: https://chromium.googlesource.com/chromium/src/+/master/docs/security/security-labels.md#TOC-Merge-labels - thanks!

Adding Merge-Request-90 so I don't overlook it in future.

Approving merge to M91, branch 4472.

Comment 23 by schwering@google.com on Mon, Apr 26, 2021, 1:45 PM EDT

Status: Fixed (was: Started)

Thanks!

Comment 24 by sheriffbot on Mon, Apr 26, 2021, 2:02 PM EDT

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

Comment 25 by Git Watcher on Mon, Apr 26, 2021, 6:26 PM EDT

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/1a33df493a17c7c66955318c8c5c1dd1f3026e62

commit 1a33df493a17c7c66955318c8c5c1dd1f3026e62
Author: Christoph Schwering <schwering@google.com>
Date: Mon Apr 26 22:25:19 2021

[Autofill] Fixed disappearing Autofill popup.

(cherry picked from commit ce5bb101c32b4e007c339aea3f9d57b91ed29e47)

~~Bug: 1200766~~
Change-Id: I72a582326c183e0cc9ad226d95cae6d118a0b7a2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2846511
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875206}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2851241
Auto-Submit: Christoph Schwering <schwering@google.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Marc Treib <treib@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#433}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/1a33df493a17c7c66955318c8c5c1dd1f3026e62/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 26 by super...@gmail.com on Mon, Apr 26, 2021, 7:48 PM EDT

Hi, Thanks for the fix! In my test it has a good perform.

And could you change the impact OS more widely? I think it's not just impact mac. Thank you again!

Comment 27 by sheriffbot on Tue, Apr 27, 2021, 12:43 PM EDT

Labels: reward-topanel

Comment 28 by schwering@google.com on Tue, Apr 27, 2021, 6:25 PM EDT

Adrian, the fix CL now lists Dev: https://chromiumdash.appspot.com/commit/ce5bb101c32b4e007c339aea3f9d57b91ed29e47. I suppose this means the CL is eligible for merge with M90, right?

Comment 29 by adetaylor@google.com on Tue, Apr 27, 2021, 6:45 PM EDT

I'll go through and approve merges for M90 a few days before the next M90 release, to give everything maximal bake time.

Comment 30 by schwering@google.com on Fri, Apr 30, 2021, 6:50 AM EDT

~~Issue 1204428~~ has been merged into this issue.

Comment 31 by adetaylor@google.com on Tue, May 4, 2021, 12:55 PM EDT

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 32 by Git Watcher on Wed, May 5, 2021, 4:05 AM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e8df881182c4c62f7079bb15a9fee2bbad4a6cda

commit e8df881182c4c62f7079bb15a9fee2bbad4a6cda
Author: Christoph Schwering <schwering@google.com>
Date: Wed May 05 08:04:37 2021

[Autofill] Fixed disappearing Autofill popup.

(cherry picked from commit ce5bb101c32b4e007c339aea3f9d57b91ed29e47)

~~Bug: 1200766~~
Change-Id: I72a582326c183e0cc9ad226d95cae6d118a0b7a2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2846511
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875206}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871611
Auto-Submit: Christoph Schwering <schwering@google.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Marc Treib <treib@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1397}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/e8df881182c4c62f7079bb15a9fee2bbad4a6cda/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 33 by Git Watcher on Thu, May 6, 2021, 10:36 AM EDT

Labels: merge-merged-4430_101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0fb5875b19f1bd5bf6228df16793c0de17595e9d

commit 0fb5875b19f1bd5bf6228df16793c0de17595e9d
Author: Christoph Schwering <schwering@google.com>
Date: Thu May 06 14:35:53 2021

[Autofill] Fixed disappearing Autofill popup.

(cherry picked from commit ce5bb101c32b4e007c339aea3f9d57b91ed29e47)

(cherry picked from commit e8df881182c4c62f7079bb15a9fee2bbad4a6cda)

~~Bug: 1200766~~
Change-Id: I72a582326c183e0cc9ad226d95cae6d118a0b7a2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2846511
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#875206}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871611
Auto-Submit: Christoph Schwering <schwering@google.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Marc Treib <treib@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1397}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2874887
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@{#3}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/0fb5875b19f1bd5bf6228df16793c0de17595e9d/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 34 by amyressler@chromium.org on Fri, May 7, 2021, 5:18 PM EDT

Labels: Release-3-M90

Comment 35 by vsavu@google.com on Mon, May 10, 2021, 9:26 AM EDT

Labels: LTS-Merge-Request-86 LTS-Security-86

Comment 36 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT

Labels: CVE-2021-30514 CVE_description-missing

Comment 37 by gianluca@google.com on Wed, May 12, 2021, 12:30 PM EDT

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 38 by amyressler@google.com on Wed, May 12, 2021, 7:11 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 39 by amyressler@chromium.org on Wed, May 12, 2021, 7:29 PM EDT

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

Comment 40 by super...@gmail.com on Fri, May 14, 2021, 7:43 AM EDT

Thank you!

Comment 41 by amyressler@google.com on Mon, May 17, 2021, 2:19 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 42 by Git Watcher on Tue, May 18, 2021, 6:54 AM EDT

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f1371cbaca0a74b81cfdd80f99825980dbb62fa0

commit f1371cbaca0a74b81cfdd80f99825980dbb62fa0
Author: Christoph Schwering <schwering@google.com>
Date: Tue May 18 10:53:20 2021

[Autofill] Fixed disappearing Autofill popup.

(cherry picked from commit ce5bb101c32b4e007c339aea3f9d57b91ed29e47)

~~Bug: 1200766~~
Change-Id: I72a582326c183e0cc9ad226d95cae6d118a0b7a2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2846511
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Marc Treib <treib@chromium.org>
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875206}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883724
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1641}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/f1371cbaca0a74b81cfdd80f99825980dbb62fa0/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc

Comment 43 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 44 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