


☆ Starred by 5 users

Owner:

mamir@chromium.org

CC:

 cfroussios@chromium.org
mahmadi@chromium.org
battre@chromium.org
kolos@chromium.org
schwering@google.com
mamir@chromium.org
koerber@google.com
ios-bugs-priority@chromium.org
ios-bugs@chromium.org
mlerman@chromium.org

Status:

Fixed (Closed)

Components:

UI>Browser>Autofill

Modified:

Sep 9, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Android, Windows, iOS, Chrome, Mac, Fuchsia, Lacros

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
reward-15000
CVE_description-submitted
M-91
Target-91
external_security_report
merge-merged-4430
merge-merged-90
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
Release-0-M92
LTS-Size-Normal
CVE-2021-30575
~~LTS-Complexity-Medium~~

Issue 1213313: Security: HeapOverflow in FillPhoneCountryCode

Reported by leccraso@gmail.com on Tue, May 25, 2021, 11:34 PM EDT

 Code

VULNERABILITY DETAILS

In function FillPhoneCountryCodeSelectControl[1], the size of field->option_contents could mismatch with the size of field->option_values. If the size of option_contents is larger than the size of option_values, the HeapOverflow will be trigger when field->option_values[i] gets accessed.

[1]. https://source.chromium.org/chromium/chromium/src/+main:components/autofill/core/browser/field_filler.cc;l=795;drc=1156b5f891de178171e71b9221a96bef1ced3d3b

VERSION

Chrome Version: stable but need a flag
Operating System: All

REPRODUCTION CASE

1. Apply the attached patch.diff to enable "kAutofillEnableAugmentedPhoneCountryCode" flag and emulates a compromised renderer.
2. \$ python -m SimpleHTTPServer
\$ out/asan/chrome --user-data-dir=/tmp/xxxx "http://localhost:8000/poc.html"

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: browser
Crash State: see asan file

CREDIT INFORMATION

Reporter credit: Leccraso and Guang Gong of 360 Alpha Lab

asan
17.0 KB [View](#) [Download](#)

patch.diff
1.5 KB [View](#) [Download](#)

poc.html
1.2 KB [View](#) [Download](#)

trigger.html
392 bytes [View](#) [Download](#)

Comment 1 by sheriffbot on Tue, May 25, 2021, 11:39 PM EDT Project Member

Labels: external_security_report

Comment 2 by adetaylor@google.com on Wed, May 26, 2021, 4:10 PM EDT Project Member

Owner: kolos@chromium.org
Cc: mamir@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-iOS OS-Lacros Pri-2
Components: UI>Browser>Autofill

Reproduced on Chrome revision 3d60439cfb36485e76a1c5bb7f513d3721b20da1, 870763, M91 branch point. Setting security impact stable, and security severity medium as an OOB read in the browser which can be triggered by a compromised renderer.

Comment 3 by [mamir@chromium.org](#) on Thu, May 27, 2021, 9:48 AM EDT Project Member
Cc: schwering@google.com

Comment 4 by [mamir@chromium.org](#) on Thu, May 27, 2021, 10:10 AM EDT Project Member
Status: Assigned (was: Unconfirmed)
Owner: mamir@chromium.org
Cc: -mamir@chromium.org

Comment 5 by [mamir@chromium.org](#) on Thu, May 27, 2021, 10:10 AM EDT Project Member
Cc: mamir@chromium.org kolos@chromium.org
[Issue-1212312](#) has been merged into this issue.

Comment 6 by [mamir@chromium.org](#) on Thu, May 27, 2021, 10:57 AM EDT Project Member
Cc: mahmadi@chromium.org cfroussios@chromium.org
[Issue-1212363](#) has been merged into this issue.

Comment 7 by [Git Watcher](#) on Thu, May 27, 2021, 1:02 PM EDT Project Member
The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+05303a33a5a31d74709ddaff9e54fed2fd0ebaa8>

commit 05303a33a5a31d74709ddaff9e54fed2fd0ebaa8
Author: Mohamed Amir Yosef <[mamir@chromium.org](#)>
Date: Thu May 27 17:01:40 2021

[Autofill] Check the size of both contents and values in FormFieldData

Details are in the linked bug.

[Bug-1212312](#)
Change-Id: I8e0a4d55ddd5c0c0ce350378fab0f282a36019f
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2922343>
Reviewed-by: Christoph Schwering <[schwering@google.com](#)>
Commit-Queue: Mohamed Amir Yosef <[mamir@chromium.org](#)>
Cr-Commit-Position: refs/heads/master@{#887197}

[modify] https://crrev.com/05303a33a5a31d74709ddaff9e54fed2fd0ebaa8/components/autofill/core/browser/field_filler.cc
[modify] https://crrev.com/05303a33a5a31d74709ddaff9e54fed2fd0ebaa8/components/autofill/core/browser/form_data_importer.cc

Comment 8 by [sheriffbot](#) on Thu, May 27, 2021, 1:04 PM EDT Project Member
Labels: M-91 Target-91

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 [sheriffbot](#) on Thu, May 27, 2021, 1:40 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 10 by [leecraso@gmail.com](#) on Thu, May 27, 2021, 1:59 PM EDT

Hi, thanks for the quick fix. But I think those should be marked as fixed, rather than be duplicated into one medium severity issue.

Comment 11 by [schwering@google.com](#) on Thu, May 27, 2021, 8:55 PM EDT Project Member

Thanks for the report! I think the three are really the different instances of the same bug (wrong loop condition of the same two fields).

Comment 12 by [leecraso@gmail.com](#) on Thu, May 27, 2021, 11:10 PM EDT

yes, it's the same pattern, but the call path is different. It seems that different CVEs will be assigned for these before:

<https://chromium-review.googlesource.com/c/chromium/src/+2440620>
<https://chromium-review.googlesource.com/c/chromium/src/+2891080>

And there seems to be a mistake in the patch:

https://chromium-review.googlesource.com/c/chromium/src/+2922343/3/components/autofill/core/browser/form_data_importer.cc
```for (size\_t i = 0; items\_count; ++i) {``` should be ```for (size\_t i = 0; i < items\_count; ++i) {```

**Comment 13** by [Git Watcher](#) on Fri, May 28, 2021, 2:40 AM EDT Project Member

The following revision refers to this bug:  
<https://chromium.googlesource.com/chromium/src/+b58aa12c8cefee013d0ab82be4b78eb053e7c439>

commit b58aa12c8cefee013d0ab82be4b78eb053e7c439  
Author: Mohamed Amir Yosef <[mamir@chromium.org](#)>  
Date: Fri May 28 06:39:38 2021

Revert "[Autofill] Check the size of both contents and values in FormFieldData"

This reverts commit 05303a33a5a31d74709ddaff9e54fed2fd0ebaa8.

Reason for revert: Created a regression in form\_data\_importer.cc

Original change's description:

> [Autofill] Check the size of both contents and values in FormFieldData  
>  
> Details are in the linked bug.  
>  
> [Bug-1212312](#)  
> Change-Id: I8e0a4d55ddd5c0c0ce350378fab0f282a36019f  
> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2922343>  
> Reviewed-by: Christoph Schwering <[schwering@google.com](#)>  
> Commit-Queue: Mohamed Amir Yosef <[mamir@chromium.org](#)>

> Cr-Commit-Position: refs/heads/master@{#887197}

[Bug-1213313](#)

Change-Id: Ia5bee585277ea7020cca982d05e10d91475defe9

No-Presubmit: true

No-Tree-Checks: true

No-Try: true

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2922886>

Auto-Submit: Mohamed Amir Yosef <[mamir@chromium.org](mailto:mamir@chromium.org)>

Bot-Commit: Rubber Stamper <[rubber-stamper@appspot.gserviceaccount.com](mailto:rubber-stamper@appspot.gserviceaccount.com)>

Commit-Queue: Mohamed Amir Yosef <[mamir@chromium.org](mailto:mamir@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#887479}

[modify] [https://crrev.com/b58aa12c8cefee013d0ab82be4b78eb053e7c439/components/autofill/core/browser/field\\_filler.cc](https://crrev.com/b58aa12c8cefee013d0ab82be4b78eb053e7c439/components/autofill/core/browser/field_filler.cc)

[modify] [https://crrev.com/b58aa12c8cefee013d0ab82be4b78eb053e7c439/components/autofill/core/browser/form\\_data\\_importer.cc](https://crrev.com/b58aa12c8cefee013d0ab82be4b78eb053e7c439/components/autofill/core/browser/form_data_importer.cc)

**Comment 14** by [mamir@chromium.org](mailto:mamir@chromium.org) on Fri, May 28, 2021, 2:51 AM EDT Project Member

**Cc:** [koerber@google.com](mailto:koerber@google.com)

**Comment 15** by [Git Watcher](#) on Fri, May 28, 2021, 8:03 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+624f194d9f2d988a7f8e450bc39f5f1120865312>

commit 624f194d9f2d988a7f8e450bc39f5f1120865312

Author: Mohamed Amir Yosef <[mamir@chromium.org](mailto:mamir@chromium.org)>

Date: Fri May 28 12:02:23 2021

[Autofill] Check the size of both contents and values in FormFieldData

Details are in the linked bug.

[Bug-1213313](#)

Change-Id: I9f018cd0d6a5820f9496a494dbb210445ae99f61

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2923844>

Auto-Submit: Mohamed Amir Yosef <[mamir@chromium.org](mailto:mamir@chromium.org)>

Reviewed-by: Matthias Körber <[koerber@google.com](mailto:koerber@google.com)>

Commit-Queue: Christoph Schwering <[schwering@google.com](mailto:schwering@google.com)>

Cr-Commit-Position: refs/heads/master@{#887493}

[modify] [https://crrev.com/624f194d9f2d988a7f8e450bc39f5f1120865312/components/autofill/core/browser/field\\_filler.cc](https://crrev.com/624f194d9f2d988a7f8e450bc39f5f1120865312/components/autofill/core/browser/field_filler.cc)

[modify] [https://crrev.com/624f194d9f2d988a7f8e450bc39f5f1120865312/components/autofill/core/browser/form\\_data\\_importer.cc](https://crrev.com/624f194d9f2d988a7f8e450bc39f5f1120865312/components/autofill/core/browser/form_data_importer.cc)

**Comment 16** by [mamir@chromium.org](mailto:mamir@chromium.org) on Mon, May 31, 2021, 4:03 AM EDT Project Member

**Cc:** [battra@chromium.org](mailto:battra@chromium.org)

**Comment 17** by [mamir@chromium.org](mailto:mamir@chromium.org) on Mon, May 31, 2021, 4:04 AM EDT Project Member

**Status:** Fixed (was: Assigned)

**Labels:** Merge-Request-92

**Comment 18** by [sheriffbot](#) on Mon, May 31, 2021, 4:07 AM EDT Project Member

**Labels:** -Merge-Request-92 Merge-Review-92 Hotlist-Merge-Review

This bug requires manual review: Reverts referenced in bugdroid comments after merge request.

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](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: govind@(Android), bindusuvama@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

**Comment 19** by [mamir@chromium.org](mailto:mamir@chromium.org) on Mon, May 31, 2021, 4:10 AM EDT Project Member

- 1- Yes, it's a security fix.
- 2- <https://chromium-review.googlesource.com/c/chromium/src/+2923844>
- 3- Yes, landed on Canary already. (93.0.4526.0)
- 4- Yes, merging to M91 would make sense. It's a safe change and addresses a security issue.
- 5- It's a security fix.
- 6- No, not a new feature.
- 7- The fix is safe and is not "not" behind a feature flag.

**Comment 20** by [sheriffbot](#) on Mon, May 31, 2021, 12:42 PM EDT Project Member

**Labels:** reward-topanel

**Comment 21** by [sheriffbot](#) on Mon, May 31, 2021, 2:00 PM EDT Project Member

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

**Comment 22** by [leecraso@gmail.com](mailto:leecraso@gmail.com) on Mon, May 31, 2021, 11:09 PM EDT

Hi, is the final decision to duplicate these issues into this medium severity issue? Some of them could leak memory by reallocating the freed space without user interaction. I think it should be high severity at least.

**uaf-asan**

27.7 KB [View](#) [Download](#)

**Comment 23** by [srinivassista@google.com](mailto:srinivassista@google.com) on Wed, Jun 2, 2021, 1:43 PM EDT Project Member

**Labels:** -Merge-Review-92 Merge-Approved-92

Merge approved for M92 branch:4515 please merge asap

Comment 24 by Git Watcher on Wed, Jun 2, 2021, 4:38 PM EDT Project Member

**Labels:** -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+be223652b6078b56540a6cb5db2d442674d0f073>

commit [be223652b6078b56540a6cb5db2d442674d0f073](#)

Author: Mohamed Amir Yosef <mamir@chromium.org>

Date: Wed Jun 02 20:36:58 2021

[Autofill] Check the size of both contents and values in FormFieldData

Details are in the linked bug.

(cherry picked from commit [624f194d9f2d988a7f8e450bc39f5f120865312](#))

[Bug-1242343](#)

Change-Id: I9f018cd0d6a5820f9496a49d4dbb210445ae99f61

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2923844>

Auto-Submit: Mohamed Amir Yosef <mamir@chromium.org>

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

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

Cr-Original-Commit-Position: refs/heads/master@{#887493}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2933900>

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

Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>

Cr-Commit-Position: refs/branch-heads/4515@{#254}

Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4c1c-refs/heads/master@{#885287}

[modify] [https://crrev.com/be223652b6078b56540a6cb5db2d442674d0f073/components/autofill/core/browser/field\\_filler.cc](https://crrev.com/be223652b6078b56540a6cb5db2d442674d0f073/components/autofill/core/browser/field_filler.cc)

[modify] [https://crrev.com/be223652b6078b56540a6cb5db2d442674d0f073/components/autofill/core/browser/form\\_data\\_importer.cc](https://crrev.com/be223652b6078b56540a6cb5db2d442674d0f073/components/autofill/core/browser/form_data_importer.cc)

Comment 25 by mamir@chromium.org on Tue, Jun 8, 2021, 10:15 AM EDT Project Member

[Issue-124266](#) has been merged into this issue.

Comment 26 by Git Watcher on Wed, Jun 9, 2021, 12:38 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+d805a11b69ccf6376a1a5e05bfe603a4481c3a5>

commit [d805a11b69ccf6376a1a5e05bfe603a4481c3a5](#)

Author: Christoph Schwering <schwering@google.com>

Date: Wed Jun 09 16:37:48 2021

[Autofill] Replaced pair of value/label vectors with vector of pairs.

[Bug-1242343](#)

Change-Id: Iab2688936636676157bdcd0b3db6f80f8a53cea

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2935277>

Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>

Reviewed-by: Mike West <mkwst@chromium.org>

Reviewed-by: Michael Bai <michaelbai@chromium.org>

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

Cr-Commit-Position: refs/heads/master@{#890810}

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/chrome/renderer/autofill/form\\_autofill\\_browser\\_test.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/chrome/renderer/autofill/form_autofill_browser_test.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/android\\_autofill/browser/form\\_field\\_data\\_android.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/android_autofill/browser/form_field_data_android.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/content/renderer/autofill\\_agent.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/content/renderer/autofill_agent.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/content/renderer/form\\_autofill\\_util.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/content/renderer/form_autofill_util.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/autofill\\_test\\_utils.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/autofill_test_utils.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/field\\_filler.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/field_filler.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/field\\_filler\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/field_filler_unittest.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_data\\_importer.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_data_importer.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_data\\_importer\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_data_importer_unittest.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_parsing/credit\\_card\\_field.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_parsing/credit_card_field.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_parsing/credit\\_card\\_field\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_parsing/credit_card_field_unittest.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_parsing/parsing\\_test\\_utils.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_parsing/parsing_test_utils.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_parsing/parsing\\_test\\_utils.h](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_parsing/parsing_test_utils.h)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_parsing/phone\\_field.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_parsing/phone_field.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form\\_parsing/phone\\_field\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/browser/form_parsing/phone_field_unittest.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/autofill\\_data\\_validation.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/autofill_data_validation.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/autofill\\_data\\_validation.h](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/autofill_data_validation.h)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form\\_data\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form_data_unittest.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form\\_field\\_data.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form_field_data.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form\\_field\\_data.h](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form_field_data.h)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form\\_field\\_data\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/form_field_data_unittest.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/mojom/autofill\\_types.mojom](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/mojom/autofill_types.mojom)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/mojom/autofill\\_types\\_mojom\\_traits.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/mojom/autofill_types_mojom_traits.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/mojom/autofill\\_types\\_mojom\\_traits.h](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/core/common/mojom/autofill_types_mojom_traits.h)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/ios/browser/autofill\\_util.mm](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/autofill/ios/browser/autofill_util.mm)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/password\\_manager/core/browser/form\\_saver\\_impl.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/password_manager/core/browser/form_saver_impl.cc)

[modify] [https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/password\\_manager/core/browser/password\\_manager\\_unittest.cc](https://crrev.com/d805a11b69ccf6376a1a5e05bfe603a4481c3a5/components/password_manager/core/browser/password_manager_unittest.cc)

Comment 27 by amyressler@google.com on Wed, Jun 23, 2021, 7:24 PM EDT Project Member

**Labels:** -reward-topanel reward-unpaid reward-15000

\*\*\* 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](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

Comment 28 by amyressler@chromium.org on Wed, Jun 23, 2021, 7:46 PM EDT Project Member

Congratulations, Leecraso and Guang Gong! The VRP Panel has decided to award you \$15,000 for this report. Nice work!

Comment 29 by amyressler@google.com on Wed, Jun 30, 2021, 5:36 PM EDT Project Member

**Labels:** -reward-unpaid reward-inprocess

Comment 30 by amyressler@chromium.org on Mon, Jul 19, 2021, 3:11 PM EDT Project Member

Labels: Release-0-M92

Comment 31 by amyressler@google.com on Mon, Jul 19, 2021, 7:16 PM EDT Project Member

Labels: CVE-2021-30575 CVE\_description-missing

Comment 32 by rzanoni@google.com on Thu, Jul 29, 2021, 5:20 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Normal LTS-Complexity-Medium

Comment 33 by amyressler@google.com on Tue, Aug 3, 2021, 3:42 PM EDT Project Member

Labels: -CVE\_description-missing CVE\_description-submitted

Comment 34 by gianluca@google.com on Thu, Aug 5, 2021, 6:22 AM EDT Project Member

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 35 by Git Watcher on Thu, Aug 5, 2021, 9:28 AM EDT Project Member

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+57b95ba2c39ae6a806cfe644ab0a5ac5ef30ac1b>

commit 57b95ba2c39ae6a806cfe644ab0a5ac5ef30ac1b

Author: Mohamed Amir Yosef <mamir@chromium.org>

Date: Thu Aug 05 13:27:38 2021

[M90-LTS][Autofill] Check the size of both contents and values in FormFieldData

Details are in the linked bug.

(cherry picked from commit 624f194d9f2d988a7f8e450bc39f5f1120865312)

[Bug=4242343](#)

Change-Id: I9f018cd0d6a5820f9496a494dbb210445ae99f61

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2923844>

Auto-Submit: Mohamed Amir Yosef <mamir@chromium.org>

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

Cr-Original-Commit-Position: refs/heads/master@{#887493}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3056955>

Reviewed-by: Jana Grill <janagrill@google.com>

Owners-Override: Jana Grill <janagrill@google.com>

Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>

Cr-Commit-Position: refs/branch-heads/4430@{#1554}

Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] [https://crrev.com/57b95ba2c39ae6a806cfe644ab0a5ac5ef30ac1b/components/autofill/core/browser/field\\_filler.cc](https://crrev.com/57b95ba2c39ae6a806cfe644ab0a5ac5ef30ac1b/components/autofill/core/browser/field_filler.cc)

[modify] [https://crrev.com/57b95ba2c39ae6a806cfe644ab0a5ac5ef30ac1b/components/autofill/core/browser/form\\_data\\_importer.cc](https://crrev.com/57b95ba2c39ae6a806cfe644ab0a5ac5ef30ac1b/components/autofill/core/browser/form_data_importer.cc)

Comment 36 by rzanoni@google.com on Thu, Aug 5, 2021, 9:46 AM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 37 by Git Watcher on Thu, Aug 5, 2021, 10:28 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+88c291f2388668bcf44d97d8259476cfc71f50ad>

commit 88c291f2388668bcf44d97d8259476cfc71f50ad

Author: Christoph Schwering <schwering@google.com>

Date: Thu Aug 05 14:26:19 2021

[M90-LTS][Autofill] Replaced pair of value/label vectors with vector of pairs.

Since <https://chromium-review.googlesource.com/c/chromium/src/+2752287>

isn't on M90, //comp/autofill is still using base::string16 instead of

std::u16string.

A few changes were made the original cl:

- changed all occurrences of std::u16string to base::string16

- keep using base::ASCIIToUTF16 where needed

- Added changes to //comp/autofill/core/browser/form\_structure.cc

and //comp/autofill/core/browser/form\_structure\_unittest.cc, not

included in the original cl (build fixes).

(cherry picked from commit d805a11b69ccfc6376a1a5e05bfe603a4481c3a5)

[Bug=4242343](#)

Change-Id: Iab2688936636676157bdcd0b3db6f0f8a53cea

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2935277>

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

Cr-Original-Commit-Position: refs/heads/master@{#890810}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3056956>

Reviewed-by: Jana Grill <janagrill@google.com>

Owners-Override: Jana Grill <janagrill@google.com>

Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>

Cr-Commit-Position: refs/branch-heads/4430@{#1559}

Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/chrome/renderer/autofill/form\\_autofill\\_browsertest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/chrome/renderer/autofill/form_autofill_browsertest.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/android/provider/form\\_field\\_data\\_android.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/android/provider/form_field_data_android.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/content/renderer/autofill\\_agent.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/content/renderer/autofill_agent.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/content/renderer/form\\_autofill\\_util.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/content/renderer/form_autofill_util.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/autofill\\_test\\_utils.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/autofill_test_utils.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/field\\_filler.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/field_filler.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/field\\_filler\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/field_filler_unittest.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_data\\_importer.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_data_importer.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_data\\_importer\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_data_importer_unittest.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_parsing/credit\\_card\\_field.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_parsing/credit_card_field.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_parsing/credit\\_card\\_field\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_parsing/credit_card_field_unittest.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_parsing/parsing\\_test\\_utils.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_parsing/parsing_test_utils.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_parsing/parsing\\_test\\_utils.h](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_parsing/parsing_test_utils.h)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_parsing/phone\\_field.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_parsing/phone_field.cc)

[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_parsing/phone\\_field\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_parsing/phone_field_unittest.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_structure.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_structure.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form\\_structure\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/browser/form_structure_unittest.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/autofill\\_data\\_validation.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/autofill_data_validation.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/autofill\\_data\\_validation.h](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/autofill_data_validation.h)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form\\_data\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form_data_unittest.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form\\_field\\_data.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form_field_data.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form\\_field\\_data.h](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form_field_data.h)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form\\_field\\_data\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/form_field_data_unittest.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/mojom/autofill\\_types.mojom](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/mojom/autofill_types.mojom)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/mojom/autofill\\_types\\_mojom\\_traits.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/mojom/autofill_types_mojom_traits.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/mojom/autofill\\_types\\_mojom\\_traits.h](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/core/common/mojom/autofill_types_mojom_traits.h)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/ios/browser/autofill\\_util.mm](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/autofill/ios/browser/autofill_util.mm)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/password\\_manager/core/browser/form\\_saver\\_impl.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/password_manager/core/browser/form_saver_impl.cc)  
[modify] [https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/password\\_manager/core/browser/password\\_manager\\_unittest.cc](https://crrev.com/88c291f2388668bcf44d97d8259476cfc71f50ad/components/password_manager/core/browser/password_manager_unittest.cc)

Comment 38 by sheriffbot on Thu, Sep 9, 2021, 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