

☆ Starred by 2 users

**Owner:**


michaeldo@chromium.org


**CC:**


adetaylor@chromium.org

jun.k...@microsoft.com

eugen...@chromium.org


 noyau@chromium.org

 bindusuvama@chromium.org

 nasko@chromium.org

ios-bugs-priority@chromium.org

ios-bugs@chromium.org

 ajuma@chromium.org

**Status:**

Fixed (Closed)

**Components:**

Mobile>iOSWeb>ScriptInjections

**Modified:**

Jan 14, 2021

**Backlog-Rank:**

----

**Editors:**

----

**EstimatedDays:**

----

**NextAction:**

----

**OS:**

iOS

**Pri:**

1

**Type:**

Bug-Security

Hotlist-Merge-Review

Security\_Impact-Stable

Security\_Severity-High

allpublic

Via-Wizard-Security

CVE\_description-submitted

M-84

merge-merged-4147

merge-merged-84

Respin-84-iOS

Release-1-M84

CVE-2020-16046

**Issue 1098606: WebFrameImpl::CallJavaScriptFunction allows child frames to inject scripts into parent.**

Reported by ahuff...@microsoft.com on Wed, Jun 24, 2020, 12:30 AM EDT Project Member

 Code

Steps to reproduce the problem:

1. Ensure autofill is enabled.
2. Navigate to parent.html.
3. An alert appears with the contents of parent.html triggered by child.html.

What is the expected behavior?

Nothing.

What went wrong?

The javascript generated by WebFrameImpl::CallJavaScriptFunction is unsafely created using the following format string.

```
std::string script =
    base::StringPrintf("__gCrWeb.message.routeMessage(%s, %s, %s)",
        encrypted_message_json.c_str(),
        encrypted_function_json.c_str(), frame_id_c_str());
```

The frame\_id\_ parameter is fully controllable by creating a new WebFrameImpl through the window.webkit.messageHandlers.FrameBecameAvailable.postMessage method. Once the new WebFrameImpl is created, autofill attempts to route a message to the new frame triggering XSS in the parent frame.

While not demonstrated in the poc this frame can be placed on a different origin allowing a user to execute javascript on any site where an iframe can be embedded.

Did this work before? N/A

Chrome version: 83.0.4103.88 Channel: stable

OS Version: 13.5.1

Flash Version:

**parent.html**  
116 bytes [View](#) [Download](#)

**child.html**  
373 bytes [View](#) [Download](#)

Comment 1 Deleted

Comment 2 by bdea@chromium.org on Wed, Jun 24, 2020, 3:47 PM EDT  
@michaeldo can you take a look at this?

Comment 3 by bdea@chromium.org on Wed, Jun 24, 2020, 3:48 PM EDT

**Owner:** michaeldo@chromium.org  
**Components:** Mobile>iOSWeb>ScriptInjections

Comment 4 by [michaeldo@chromium.org](mailto:michaeldo@chromium.org) on Wed, Jun 24, 2020, 6:10 PM EDT

Status: Started (was: Unconfirmed)

Thank you for the discovery, repo steps and PoC.

I have uploaded a fix at [crrev.com/c/2264468](https://crrev.com/c/2264468)

Comment 5 by [bdea@chromium.org](mailto:bdea@chromium.org) on Wed, Jun 24, 2020, 6:46 PM EDT

Labels: Security\_Impact-Head M-85 Security\_Severity-Medium

Comment 6 by [michaeldo@chromium.org](mailto:michaeldo@chromium.org) on Wed, Jun 24, 2020, 6:51 PM EDT

Cc: eugen...@chromium.org

+ CL reviewer

Comment 7 by [ahuff...@microsoft.com](mailto:ahuff...@microsoft.com) on Wed, Jun 24, 2020, 8:23 PM EDT Project Member

Wow! Quick turnaround. Would you mind clarifying the severity? The bug can execute a script on behalf of another origin. This is mentioned as one of the High severity bugs in <https://chromium.googlesource.com/chromium/src/+master/docs/security/severity-guidelines.md#TOC-High-severity>. Two Google products this can be applied to are [translate.google.com](https://translate.google.com) and [sites.google.com](https://sites.google.com).

Comment 8 by [ajuma@chromium.org](mailto:ajuma@chromium.org) on Thu, Jun 25, 2020, 10:38 AM EDT

Question about the patch: the patch disallows non-hex frame ids, but what happens if the PoC is changed to use '12345' as crwFrameld instead of 'foobar'?

Comment 9 by [michaeldo@chromium.org](mailto:michaeldo@chromium.org) on Thu, Jun 25, 2020, 11:18 AM EDT

In the patch, it's the entire crwFrameld string from the message dictionary that is validated to be only containing hex chars, not only the 'foobar' part. The hex validation ensures that there are no characters which could escape from the frameld when it is used later to build JS strings to execute.

Comment 10 by [sheriffbot](mailto:sheriffbot) on Thu, Jun 25, 2020, 2:20 PM EDT

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security\_Impact or Security\_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 11 by [sheriffbot](mailto:sheriffbot) on Thu, Jun 25, 2020, 2:42 PM EDT

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 12 by [bugdroid](mailto:bugdroid) on Thu, Jun 25, 2020, 3:30 PM EDT

Status: Fixed (was: Started)

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+37bcc228e1089bb07e37c9137bd03437b7c4de7>

commit 37bcc228e1089bb07e37c9137bd03437b7c4de7

Author: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Date: Thu Jun 25 19:29:27 2020

[IOS] Ignore invalid framelds

Additionally, update tests to use correctly formatted frame ids.

~~Fixed-1008696~~

Change-Id: I0d0b9cfa473d20433c228863af3a434ff50b5f1

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2264468>

Commit-Queue: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Auto-Submit: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Reviewed-by: Eugene But <[eugenebut@chromium.org](mailto:eugenebut@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#782598}

[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/chrome/browser/autofill/form\\_suggestion\\_controller\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/chrome/browser/autofill/form_suggestion_controller_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/chrome/browser/ui/autofill/manual\\_fill\\_full\\_card\\_requester\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/chrome/browser/ui/autofill/manual_fill_full_card_requester_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/chrome/browser/web/font\\_size\\_tab\\_helper\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/chrome/browser/web/font_size_tab_helper_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/find\\_in\\_page/find\\_in\\_page\\_manger\\_impl\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/find_in_page/find_in_page_manger_impl_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/find\\_in\\_page/find\\_in\\_page\\_request\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/find_in_page/find_in_page_request_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/js\\_messaging/web\\_frame\\_util\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/js_messaging/web_frame_util_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/js\\_messaging/web\\_frames\\_manager\\_impl.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/js_messaging/web_frames_manager_impl.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/js\\_messaging/web\\_frames\\_manager\\_impl\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/js_messaging/web_frames_manager_impl_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/public/test/fakes/fake\\_web\\_frame.cc](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/public/test/fakes/fake_web_frame.cc)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/public/test/fakes/fake\\_web\\_frame.h](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/public/test/fakes/fake_web_frame.h)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/web\\_state/web\\_state\\_impl\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/web_state/web_state_impl_unittest.mm)  
[modify] [https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/web\\_view/internal/autofill/cwv\\_autofill\\_controller\\_unittest.mm](https://crrev.com/37bcc228e1089bb07e37c9137bd03437b7c4de7/ios/web/web_view/internal/autofill/cwv_autofill_controller_unittest.mm)

Comment 13 by [sheriffbot](mailto:sheriffbot) on Thu, Jun 25, 2020, 4:13 PM EDT

Labels: Merge-TBD

This release blocking issue appears to be targeted for M85, which has already branched. Because this issue was marked as fixed after branch point, a merge of any CLs which landed on or after June 25 may be required. Please review whether or not any CLs should be merged ASAP, and if a merge is necessary apply the label Merge-Request-85 to begin the merge review process. If no merge is required, please simply remove the Merge-TBD label.

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

Comment 14 by [sheriffbot](mailto:sheriffbot) on Fri, Jun 26, 2020, 3:06 PM EDT

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

Comment 15 by [michaeldo@chromium.org](mailto:michaeldo@chromium.org) on Sat, Jun 27, 2020, 12:15 AM EDT

Labels: -Merge-TBD

This change made it into M85, no merge needed.

Comment 16 by [ahuff...@microsoft.com](mailto:ahuff...@microsoft.com) on Wed, Jul 15, 2020, 3:49 PM EDT Project Member

Cc: jun.k...@microsoft.com

Comment 17 by [jun.k...@microsoft.com](mailto:jun.k...@microsoft.com) on Wed, Jul 15, 2020, 3:57 PM EDT

**Cc:** nasko@chromium.org

**Labels:** -Security\_Impact-Head Security\_Impact-Stable

The PoC works on Chrome for iOS 83, so this affects stable.

nasko@, this is a UXSS bug. This is a High severity bug IMO. WDYT?

[Comment 18](#) by [nasko@chromium.org](#) on Wed, Jul 15, 2020, 4:59 PM EDT

**Cc:** adetaylor@chromium.org

Adding adetaylor@, who manages our security guidelines and can probably help faster than me here.

[Comment 19](#) by [adetaylor@chromium.org](#) on Wed, Jul 15, 2020, 5:46 PM EDT

**Cc:** bindusuvarna@chromium.org

**Labels:** -Security\_Severity-Medium -ReleaseBlock-Stable -M-85 M-84 Security\_Severity-High

I agree this seems to impact stable so adjusting flags appropriately. I also agree that this appears to be valid UXSS so I'll rate it as High.

Sheriffbot will shortly add an M84 merge request. As a high severity security bug, we'd normally merge this back to the next regular stable refresh, but we don't always make such regular iOS refreshes. bindusuvarna@, would you expect to make an M84 security refresh for iOS?

[Comment 20](#) by [bindusuvarna@chromium.org](#) on Thu, Jul 16, 2020, 4:57 PM EDT

adetaylor@ Currently, there isn't any planned respin for M84. I am marking this as RBS so it's included for when we have one. If there isn't any planned respin then is a respin required for this?

[Comment 21](#) by [adetaylor@chromium.org](#) on Thu, Jul 16, 2020, 10:47 PM EDT

**Labels:** Merge-Request-84

We do not typically respin \_just\_ for a high severity fix, but then again it's an unusual situation because on other platforms we have a train coming along every two weeks. It's unusual for us to have an iOS-only fix like this.

I must say this does feel quite serious. It could be possible for a malicious ad to steal data or credentials from a website in which they're embedded. I think on the whole, I'd at least ask, what would it take to get out an extra release sometime sooner than 6 weeks away?

[Comment 22](#) by [sheriffbot](#) on Thu, Jul 16, 2020, 10:50 PM EDT

**Labels:** -Merge-Request-84 Merge-Review-84 Hotlist-Merge-Review

This bug requires manual review: Request affecting a post-stable build  
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 master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: govind@ (Android), bindusuvarna@ (iOS), marinakz@ (ChromeOS), pbommana@ (Desktop)

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

[Comment 23](#) by [michaeldo@chromium.org](#) on Fri, Jul 17, 2020, 11:57 AM EDT

Just a note from my review of why it didn't get into M-84: It sounds like this should have been marked for M-84 earlier to prevent a respin. (In [#c5](#) it was only marked M-85.) Note the report date of this bug was right around stable cut per <https://chromiumdash.appspot.com/schedule>

[Comment 24](#) by [adetaylor@google.com](#) on Mon, Jul 20, 2020, 1:49 PM EDT

**Labels:** -Merge-Review-84 Merge-Approved-84

Approving merge to M84. Please merge to branch 4147, assuming no related problems have shown up in Canary. The plan is indeed probably to make an iOS respin, but it may be a few weeks away just to ensure we can mop up any other high severity bugs which we need to ship as well.

[Comment 25](#) by [bugdroid](#) on Tue, Jul 21, 2020, 6:48 PM EDT

**Labels:** -merge-approved-84 merge-merged-84 merge-merged-4147

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+9c80a23e06c64a9c742a191f02b19eebf73a2aaf>

commit [9c80a23e06c64a9c742a191f02b19eebf73a2aaf](#)

Author: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Date: Tue Jul 21 22:47:07 2020

[iOS] Ignore invalid framelds

Additionally, update tests to use correctly formatted frame ids.

(cherry picked from commit [37bcc228e1089bb07e37c9137bd03437b7c4de7](#))

[Fixed: 1008606](#)

Change-Id: [I0d0b9cfa473d20433c228863af3a434ff50b5f1](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2264468>

Commit-Queue: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Auto-Submit: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Reviewed-by: Eugene But <[eugenebut@chromium.org](mailto:eugenebut@chromium.org)>

Cr-Original-Commit-Position: refs/heads/master@{#782598}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2309555>

Reviewed-by: Mike Dougherty <[michaeldo@chromium.org](mailto:michaeldo@chromium.org)>

Cr-Commit-Position: refs/branch-heads/4147@{#917}

Cr-Branched-From: [16307825352720ae04d898f37ef54549ad68b606](#)-refs/heads/master@{#768962}

[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/chrome/browser/autofill/form\\_suggestion\\_controller\\_unittest.mm](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/chrome/browser/autofill/form_suggestion_controller_unittest.mm)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/chrome/browser/ui/autofill/manual\\_fill/full\\_card\\_requester\\_unittest.mm](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/chrome/browser/ui/autofill/manual_fill/full_card_requester_unittest.mm)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/chrome/browser/web/font\\_size\\_tab\\_helper\\_unittest.mm](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/chrome/browser/web/font_size_tab_helper_unittest.mm)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/find\\_in\\_page/find\\_in\\_page\\_manger\\_impl\\_unittest.mm](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/find_in_page/find_in_page_manger_impl_unittest.mm)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/public/test/fakes/fake\\_web\\_frame.cc](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/public/test/fakes/fake_web_frame.cc)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/public/test/fakes/fake\\_web\\_frame.h](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/public/test/fakes/fake_web_frame.h)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/web\\_state/web\\_state\\_impl\\_unittest.mm](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web/web_state/web_state_impl_unittest.mm)  
[modify] [https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web\\_view/internal/autofill/cwv\\_autofill\\_controller\\_unittest.mm](https://crrev.com/9c80a23e06c64a9c742a191f02b19eebf73a2aaf/ios/web_view/internal/autofill/cwv_autofill_controller_unittest.mm)

[Comment 26](#) by [bindusuvama@chromium.org](mailto:bindusuvama@chromium.org) on Tue, Jul 28, 2020, 11:49 AM EDT

**Labels:** Respin-84-IOS

[Comment 27](#) by [bindusuvama@chromium.org](mailto:bindusuvama@chromium.org) on Tue, Jul 28, 2020, 12:55 PM EDT

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

[Comment 28](#) by [bindusuvama@chromium.org](mailto:bindusuvama@chromium.org) on Tue, Aug 11, 2020, 10:45 AM EDT

A friendly reminder to initiate postmortem for this bug which was part of the M84 respin.

Instructions for the postmortem can be found at [go/chrome-postmortems](https://go/chrome-postmortems)

SLO for postmortems is 2 weeks per [go/chrome-postmortems](https://go/chrome-postmortems). If this postmortem is complete, please mark as Fixed for review. If not, please take time to finish it. After 2 weeks, memory fades and crucial information regarding this issue could be lost.

[Comment 29](#) by [sheriffbot](#) on Fri, Oct 2, 2020, 3:01 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

[Comment 30](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Tue, Dec 15, 2020, 2:51 PM EST

**Labels:** Release-1-M84 relnotes\_update\_needed

[Comment 31](#) by [amyressler@google.com](mailto:amyressler@google.com) on Tue, Jan 12, 2021, 12:10 PM EST

**Labels:** CVE-2020-16046 CVE\_description-missing

[Comment 32](#) by [amyressler@google.com](mailto:amyressler@google.com) on Thu, Jan 14, 2021, 5:02 PM EST

**Labels:** -CVE\_description-missing -relnotes\_update\_needed CVE\_description-submitted