☆ Starred by 3 users

Owner:	schwering@google.com
CC:	adetaylor@chromium.org battre@chromium.org monamohanty@google.com mustaq@chromium.org nepper@chromium.org schwering@google.com amyressler@chromium.org mamir@chromium.org koerber@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill Blink>Input>PointerLock
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-94
Target-93
M-96
Target-96
FoundIn-92
Security_Impact-Extended
Release-0-M98
CVE-2022-0467

Issue 1239496: Security: Pointer lock can be used to bypass mouse movement/keyboard input requirements for autofill

Reported by alesa...@alesandroortiz.com on Fri, Aug 13, 2021, 2:09 AM EDT

Code

VULNERABILITY DETAILS

A page can use a carefully-sized popup combined with a pointer lock to force the user to select an autofill item with three consecutive clicks, without moving their mouse or pressing keyboard keys.

Normally Chrome requires an intentional selection by the user, either by moving the mouse over an autofill item or using the keyboard to select an autofill item.

The PoC works because requesting pointer lock in a small window will set the cursor to approximately the center of the content area while pointer lock is enabled. If the cursor location coincides with an autofill prompt item, the item will be highlighted, therefore an attacker can arrange the page so the autofill prompt is shown where the cursor is expected. The autofill prompt also accept clicks while pointer lock is enabled, so the user is able to click on the forced selection. With this last click, the browser provides the autofill data to the page.

A user who clicks more slowly or is more observant may stop prior to the last click. However, because of the pointer lock it may be initially confusing on how to escape, and they may accidentally select the item. If a user tried to move their mouse and click repeatedly to find their cursor (which may occur instinctively despite browser providing escape instructions moments before), they're very likely to accidentally select an autofill item since the prompt covers most of the window and mouse movements are bounded to the window.

I've tested this with addresses (which includes name + email) and credit cards. For sample input, see the video recording.

VERSION

Chrome Version: 92.0.4515.131 (Official Build) (64-bit) (cohort: Stable), 94.0.4605.0 Canary
Operating System: Windows 10 OS Version 2009 (Build 19042.1110)

REPRODUCTION CASE

PoC for address:
Prerequisite: Have at least one address with email address in chrome://settings/addresses
1. Navigate to https://alesandroortiz.com/security/chromium/autofill-pointer-lock.html
2. Click the same place three times in a row, anywhere in the page.

PoC for credit card:
Prerequisite: Have at least one credit card in chrome://settings/payments
1. Navigate to https://alesandroortiz.com/security/chromium/autofill-pointer-lock.html?creditcard
2. (Same as prior PoC, click three times in a row)

For all PoCs:
Observed: Autofilled data is provided to page, because pointer lock allows page to select an autofill item by moving the cursor over the autofill prompt, without any mouse movement or keyboard input.
Expected: Autofilled data is *not* provided to page, because page cannot select an autofill item without user intentionally moving mouse or using keyboard to select item.

CREDIT INFORMATION

Reporter credit: Alesandro Ortiz <https://AlesandroOrtiz.com>

autofill-pointer-lock.mp4
1.4 MB View Download

autofill-pointer-lock.html
1016 bytes View Download

autofill-pointer-lock-popup.html
2.2 KB View Download

Comment 1 by sheriffbot on Fri, Aug 13, 2021, 2:13 AM EDT Project Member

Labels: external_security_report

Comment 2 by wfh@chromium.org on Fri, Aug 13, 2021, 5:13 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: mamir@chromium.org
Cc: schwering@google.com koerber@google.com
Labels: Security_Severity-Medium FoundIn-92 OS-Chrome OS-Linux OS-Windows OS-Lacros Pri-1
Components: UI>Browser>Autofill Blink>Input>PointerLock

Thanks for your report, I'm not sure if this is an issue with pointerlock or one with autofill :) It seems perhaps the autofill UI shouldn't accept clicks if pointerlock is enabled but I wouldn't know what kind of use-cases that change would break.

I'm adding some folks from the teams to take a look.

Comment 3 by sheriffbot on Fri, Aug 13, 2021, 5:15 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 4 by sheriffbot on Sat, Aug 14, 2021, 12:51 PM EDT Project Member

Labels: M-93 Target-93

Setting milestone and target because of medium severity.

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

Comment 5 by mamir@chromium.org on Mon, Aug 16, 2021, 5:55 AM EDT Project Member

I have looked into this bug.
The bug doesn't repro on Mac or Linux.
It repros only on Windows.
On Mac and Linux, PointerLock does lock the pointer, and the user cannot move it to select an item,
However on Windows, the user is able to move the pointer!

This looks like a PointerLock issue to me.

Comment 6 by mamir@chromium.org on Mon, Aug 16, 2021, 6:36 AM EDT Project Member

Owner: jameshollyer@chromium.org
Cc: mamir@chromium.org

jameshollyer@
Could you please lock in this?
Specifically the difference in behavior between Mac/Linux and Windows?
On Windows, I am able to move the pointer even after PointerLock was requested.

Comment 7 by alesa...@alesandroortiz.com on Mon, Aug 16, 2021, 11:10 AM EDT

#c5: Do you mean the page (not the user) is able to move the pointer while pointer lock is enabled?

For this report it doesn't matter if user can move pointer, what matters is the page repositions pointer to a predictable location, *and* autofill prompts can be interacted with while pointer lock is enabled (as noted in #c2).

I agree with #c2 that the main issue here is the autofill prompts (and any other browser UI) should not allow interactions while pointer lock is enabled. Also unsure on which side (browser UI vs. pointer lock) this would need to be implemented.

Comment 8 by mamir@chromium.org on Mon, Aug 16, 2021, 11:22 AM EDT Project Member

On Mac and Linux, I wasn't able to select an item from the dropdown with the mouse. I don't even see a pointer.

On Windows however, I was able to move and click the mouse.

I hope jameshollyer@ can clarify more here what does "PointerLock" entail.

Comment 9 by sheriffbot on Mon, Aug 16, 2021, 1:12 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 10 by jameshollyer@chromium.org on Wed, Aug 18, 2021, 7:12 PM EDT Project Member

Owner: mustaq@chromium.org

On Windows when the pointer is locked we basically hide the cursor, then constantly reset the pointer location to the center of the page. The key here is that all pointer events(including click) should be routed to the element that holds the lock so you should not be able to click on anything you should not be able to click on anything.

I only worked on Pointer Lock to add the unadjusted movement capability. Mustaq and his team own this API.

Comment 11 by sheriffbot on Fri, Aug 27, 2021, 12:21 PM EDT Project Member

mustaq: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 12 by sheriffbot on Sat, Sep 11, 2021, 12:21 PM EDT Project Member

mustaq: Uh oh! This issue still open and hasn't been updated in the last 29 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 13 by mustaq@chromium.org on Mon, Sep 13, 2021, 4:20 PM EDT Project Member

Labels: -OS-Linux -OS-Chrome -OS-Lacros

The root cause here is that the auto-fill dialog is not aware of an active pointer-lock, and a click through a hidden+locked mouse cursor is treated as a click on the auto-fill dialog if the coordinates are correct.

The repro works as follows:
A. First click open a small window around the click position so that subsequent clicks to the opened window. The window size is made small enough so that the same click position falls within the auto-fill dialog for that small window.
B. The second click goes to the small window and locks the mouse pointer there.
C. The third click selects an auto-fill option.

This didn't repro for me on Linux or CrOS, and #c8 mentioned the same about Mac.

Comment 14 by mustaq@chromium.org on Mon, Sep 13, 2021, 4:28 PM EDT Project Member

Owner: mamir@chromium.org
Cc: mustaq@chromium.org

I reached the same conclusion as wfh@ above: making auto-fill dialog not responding to locked mouse seems like a logical fix here. But I find the repro not very easily reproducible without the user's notice, so I think P2 is the right priority here.

Assigning the bug back to mamir@ because I don't know much about autofill UI. I will be happy to help with pointer-lock state related question.

Comment 15 by sheriffbot on Wed, Sep 22, 2021, 12:22 PM EDT Project Member

Labels: -M-93 Target-94 M-94

Comment 16 by alesa...@alesandroortiz.com on Thu, Nov 11, 2021, 10:51 PM EST

Friendly ping: Any updates on this issue?

Comment 17 by mamir@chromium.org on Fri, Nov 12, 2021, 8:47 AM EST Project Member

Owner: schwering@google.com

Handing over to Chris!

Comment 18 by sheriffbot on Mon, Nov 15, 2021, 12:22 PM EST Project Member

Labels: -M-94 Target-96 M-96

Comment 19 by schwering@google.com on Wed, Nov 24, 2021, 6:59 AM EST Project Member

Cc: battre@chromium.org

Comment 20 by Git Watcher on Wed, Nov 24, 2021, 2:31 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/72ea510dc8941021f255a8b65d9f698c364c36b4

commit 72ea510dc8941021f255a8b65d9f698c364c36b4
Author: Christoph Schwering <schwering@google.com>
Date: Wed Nov 24 19:30:23 2021

[Autofill] Hide Autofill popup if the mouse pointer is locked.

This CL hides the Autofill popup when the underlying frame holds a
pointer lock.

~~Bug: 1239496~~
Change-Id: I978963775c2b0f00f88b167e00f918172bd1a955
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3297919
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Dominic Battré <battre@chromium.org>
Commit-Queue: Christoph Schwering <schwering@google.com>
Cr-Commit-Position: refs/heads/main@{#945063}

[modify]
https://crrev.com/72ea510dc8941021f255a8b65d9f698c364c36b4/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc
[modify]
https://crrev.com/72ea510dc8941021f255a8b65d9f698c364c36b4/components/autofill/core/browser/ui/popup_types.h
[modify]
https://crrev.com/72ea510dc8941021f255a8b65d9f698c364c36b4/chrome/browser/ui/autofill/autofill_popup_controller_impl.h

Comment 21 by schwering@google.com on Wed, Nov 24, 2021, 3:13 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 22 by schwering@google.com on Wed, Nov 24, 2021, 3:15 PM EST Project Member

Cc: monamohanty@google.com nepper@chromium.org

CC PMs (we discussed this bug and the fix today).

Comment 23 by alesa...@alesandroortiz.com on Wed, Nov 24, 2021, 7:39 PM EST

schwering@: Thanks for landing the fix. While trying to verify on ASan (too impatient to wait for tomorrow's Canary), I encountered a couple of potentially new stability issues. These *might* be pre-existing issues that could already be triggered in other ways, but the fix made it possible to trigger them with the PoCs below.

On ASan 945069 (next build after fix) through 945154 (latest at time of comment), the two issues below repro. On ASan 945062 (build immediately prior to fix) neither of the issues repro using PoCs below.

ASan build used for stack traces: https://commondatastorage.googleapis.com/chromium-browser-asan/index.html?prefix=win32-release_x64/asan-win32-release_x64-945154

== Issue 1: CHECK when mouse is over a highlighted autofill item and pointer lock is requested ==

Steps to reproduce:
1. Navigate to CHECK PoC: https://aogarantiza.com/chromium/crbug-1239496-CHECK.html
2. Click near top-left of page to trigger autofill prompt
3. Move mouse over the autofill item so it's highlighted (but do not click on it)
4. Wait ~2s after step 2 for page to request pointer lock

Observed: This CHECK fails:
https://source.chromium.org/chromium/chromium/src/+/main:ui/views/widget/root_view.cc;l=621;drc=ac80ceefd0c6383d3136c9dc568ec02927ec15e0

For some reason this is difficult to reproduce if the pointer lock is requested within 1s of performing step 2. Unsure if that's relevant to bug or an ASan quirk.

```
[668:11720:1124/190600.515:FATAL:root_view.cc(621)] Check failed: mouse_move_handler_.
Backtrace:
        base::debug::CollectStackTrace [0x00007FF988B52BF2+18]
(C:\b\s\w\ir\cache\builder\src\base\debug\stack_trace_win.cc:305)
        base::debug::StackTrace::StackTrace [0x00007FF98897B46A+26]
(C:\b\s\w\ir\cache\builder\src\base\debug\stack_trace.cc:197)
        logging::LogMessage::~LogMessage [0x00007FF9889B38DC+860] (C:\b\s\w\ir\cache\builder\src\base\logging.cc:587)
        logging::LogMessage::~LogMessage [0x00007FF9889B6EE0+16] (C:\b\s\w\ir\cache\builder\src\base\logging.cc:581)
        views::internal::RootView::OnMouseExited [0x00007FF98B21EC83+635]
(C:\b\s\w\ir\cache\builder\src\ui\views\widget\root_view.cc:621)
        views::Widget::OnMouseEvent [0x00007FF9888357C6+2482]
(C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1567)
        ui::EventDispatcher::DispatchEvent [0x00007FF98973B99A+216]
(C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:191)
```

(see attached check-asan.log for full backtrace)

== ~~Issue 2~~: NULL read immediately after second click in original PoC ==

Steps to reproduce:
1. Navigate to https://alesandroortiz.com/security/chromium/autofill-pointer-lock.html
2. Click the same place *twice* times in a row, anywhere in the page. (issue repros on second click; in other words, the first click on the popup)

Observed: NULL read per ASan.

I've made sure my mouse is not actually moving while reproducing, so unsure why OnMouseMoved is being called. Perhaps the pointer lock request is triggering that method.

```
==2544==ERROR: AddressSanitizer: access-violation on unknown address 0x000000000000 (pc 0x7ff98b202866 bp 0x009f5e3fe270 sp 0x009f5e3fe200 T0)
==2544==The signal is caused by a READ memory access.
==2544==Hint: address points to the zero page.
==2544==WARNING: Failed to use and restart external symbolizer!
    #0 0x7ff98b202865 in views::internal::RootView::OnMouseMoved C:\b\s\w\ir\cache\builder\src\ui\views\widget\root_view.cc:577
    #1 0x7ff98881dfa5 in views::Widget::OnMouseEvent C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1567
    #2 0x7ff989720219 in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:190
```

(see attached null-read-asan.log for full backtrace)

check-asan.log
8.4 KB View Download

null-read-asan.log
5.3 KB View Download

Comment 24 by alesa...@alesandroortiz.com on Wed, Nov 24, 2021, 7:42 PM EST

NULL read occurs here per stack trace:
https://source.chromium.org/chromium/chromium/src/+/main:ui/views/widget/root_view.cc;l=577;drc=ac80ceefd0c6383d3136c9dc568ec02927ec15e0

Comment 25 by schwering@google.com on Wed, Nov 24, 2021, 10:46 PM EST Project Member

Thanks a lot! That's very interesting.

Only had a quick look at the stack traces so far. It looks like:
- the first issue happens before the Autofill popup would be hidden if it were even displayed.
- the second issue may be a lifecycle issue in the popup.

I think the fix CL from #c20 is sound. Anyway, I'll try to take a closer look tomorrow.

Comment 26 by sheriffbot on Thu, Nov 25, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 27 by sheriffbot on Thu, Nov 25, 2021, 1:41 PM EST Project Member

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

Comment 28 by schwering@google.com on Thu, Nov 25, 2021, 10:15 PM EST Project Member

Re #c23: I can't repro either of the issues (tried with the linked ASan build as well as local debug-but-not-ASan builds on

Linux and Windows).

Can you reproduce the issues with an earlier ASan build that does not contain the patch from #c20 if, right after the Autofill popup occurs, you press Escape? The reason I'm asking: Escape hides the Autofill popup, and the patch does pretty much the same as pressing Escape: it hides the popup if the frame holds a pointer lock and either (a) the popup is about to be shown or (b) a suggestion is selected (= mouse moves over a row) or (c) a suggestion is accepted (= mouse clicks on a row) or (d) a suggestion is removed (= DEL is pressed while a row is selected). Conditions (b)–(d) can be exactly replicated with Escape. Only Condition (a) is not reproducible with Escape because the popup is not even shown.

It looks to me like the issues are surfaced by #c20 but have different causes, so perhaps it's worth filing one or two separate bugs about them (if so, please CC me). In any case, I'll give it another try with a fresh ASan build tomorrow.

Comment 29 by alesa...@alesandroortiz.com on Mon, Nov 29, 2021, 6:37 PM EST

Today on ASan 946147 (latest), it took a couple of tries and maybe some mouse movement, but both issues still repro most of the time for me. On 98.0.4737.0 Canary, the CHECK crash also repros most of the time.

> Can you reproduce the issues with an earlier ASan build that does not contain the patch from #c20 if, right after the Autofill popup occurs, you press Escape?

No, on ASan 945062 I'm unable to repro either issue and on 98.0.4710.4 Dev I'm unable to repro CHECK crash. However, I concur with you that given the correct conditions both issues should be reproducible pre-patch. Unfortunately having a difficult time identifying those conditions. The reasoning in #c28 ("patch does pretty much the same as pressing Escape") is also why I think this is a pre-existing issue.

FWIW, I'm also unable to repro either issue post-patch by pressing Escape without pointer lock request, so there must be additional conditions that are somehow met by requesting pointer lock. Tested this using https://aogarantiza.com/chromium/crbug-1239496-CHECK-b.html which is same CHECK PoC from #c23 but without pointer lock request, using same Canary and ASan builds at beginning of comment.

Will file new crbugs for both issues and request that you be CC'd (I cannot edit CC list).

Comment 30 by alesa...@alesandroortiz.com on Mon, Nov 29, 2021, 7:23 PM EST

Filed issue 1274911 and requested that schwering be CC'd. Filed as security issue so visibility would be restricted, because:
* it uses same PoCs as this crbug
* the crbug associated with the commit which added the CHECK is restricted, so unsure if it had security implications (commit 43dc9613e9badb5e0c6a11d25106271d2f23899f)
* the NULL read conditions seem basically the same as the CHECK conditions, but that code path does not have CHECKs.

Comment 31 by Git Watcher on Sat, Dec 11, 2021, 4:42 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/cf3e0d913e2374e2d783ceecbccc4b400d26fa39

commit cf3e0d913e2374e2d783ceecbccc4b400d26fa39
Author: Christoph Schwering <schwering@google.com>
Date: Wed Dec 08 03:50:33 2021

[Autofill] Check for self-destruction after selecting a suggestions.

This UAF was introduced in crrev.com/c/3297919 by hiding the popup
in SetSelectedLine() if the window holds a pointer lock. Since hiding

the popup deletes the popup, |this| must not be accessed afterwards.

This CL is a quick fix that adds checks after calling SetSelectedLine().
The followup CLs will make this and other checks for weak_this
redundant: crrev.com/c/3317979, crrev.com/c/3318297.

~~Bug: 1276850~~, ~~1239496~~
Change-Id: I79ce4df48ae969ba13033640f2ac2ac8c322373b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3318616
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Auto-Submit: Christoph Schwering <schwering@google.com>
Commit-Queue: Christoph Schwering <schwering@google.com>
Cr-Commit-Position: refs/heads/main@{#949363}

[modify]
https://crrev.com/cf3e0d913e2374e2d783ceecbccc4b400d26fa39/chrome/browser/ui/autofill/autofill_popup_controller_impl.cc
[modify]
https://crrev.com/cf3e0d913e2374e2d783ceecbccc4b400d26fa39/chrome/browser/ui/autofill/autofill_popup_controller_impl.h

Comment 32 by alesa...@alesandroortiz.com on Sun, Dec 12, 2021, 6:28 PM EST

There's no relationship between #c23 (filed as issue 1274911) and the commits referenced in #c31, correct? The spinoff issue doesn't seem fixed on 99.0.4762.0 Canary or ASan 950893 which have all three commits, so I'm guessing not related.

Comment 33 by schwering@google.com on Sun, Dec 12, 2021, 7:33 PM EST Project Member

That's right, #c31 is unrelated to #c23 / issue 1274911.

Comment 34 by alesa...@alesandroortiz.com on Thu, Jan 20, 2022, 5:24 PM EST

Will fix from #c20 be merged into Stable? Per https://chromiumdash.appspot.com/commit/72ea510dc8941021f255a8b65d9f698c364c36b4 it's in Canary+Dev+Beta, but not Stable. Not sure if it also needs to be merged elsewhere.

Comment 35 by schwering@google.com on Fri, Jan 21, 2022, 9:36 AM EST Project Member

Adrian, should we merge the fix [1] to 97?

If so, we also need to merge the fix [2] of ~~issue 1276850~~, which I unfortunately had introduced in [1].

Thanks for the pointer, Alesandro.

[1] https://chromium-review.googlesource.com/c/chromium/src/+/3318616
[2] https://chromium-review.googlesource.com/c/chromium/src/+/3318616

Comment 36 by schwering@google.com on Fri, Jan 21, 2022, 9:37 AM EST Project Member

Cc: adetaylor@chromium.org

Adrian, please take a look at #c35.

Comment 37 by adetaylor@chromium.org on Fri, Jan 21, 2022, 10:47 AM EST Project Member

Cc: amyressler@chromium.org

As this bug is rated medium severity we'd normally merge its fix to beta, but not to stable/extended stable.

Comment 38 by amyressler@chromium.org on Fri, Jan 21, 2022, 12:44 PM EST Project Member

This fix is already in M98, and will go out with the first stable release of M98, which is sufficient and consistent for medium severity issues, so we should be good here.

Comment 39 by amyressler@chromium.org on Fri, Jan 21, 2022, 12:46 PM EST Project Member

(premature submit)...and is already shipped in beta, of course

Comment 40 by amyressler@chromium.org on Mon, Jan 31, 2022, 7:45 PM EST Project Member

Labels: Release-0-M98

Comment 41 by amyressler@google.com on Tue, Feb 1, 2022, 12:43 PM EST Project Member

Labels: CVE-2022-0467 CVE_description-missing

Comment 42 by amyressler@google.com on Thu, Feb 17, 2022, 6:34 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 43 by amyressler@chromium.org on Thu, Feb 17, 2022, 6:51 PM EST Project Member

Congratulations, Alesandro! The VRP Panel has decided to award you $3,000 for this report. Thank you for reporting this issue to us and your patience while we resolved this issue.

Comment 44 by amyressler@google.com on Fri, Feb 18, 2022, 2:58 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 45 by alesa...@alesandroortiz.com on Mon, Feb 21, 2022, 7:00 PM EST

Thanks for the reward!

Comment 46 by sheriffbot on Thu, Mar 3, 2022, 1:29 PM EST 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

Comment 47 by amyressler@google.com on Tue, Apr 5, 2022, 4:07 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 48 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:28 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing