☆ Starred by 4 users

Owner:	mamir@chromium.org
CC:	adetaylor@chromium.org kavvaru@chromium.org battre@chromium.org schwering@google.com amyressler@chromium.org mamir@chromium.org koerber@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Build
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
Triaged-ET
CVE_description-submitted
external_security_report
M-96
reward-7000
FoundIn-96
Security_Impact-Extended
merge-merged-4692
merge-merged-97
LTS-NotApplicable-96
merge-merged-4758
merge-merged-98
Needs-Triage-M99
Release-0-M97
CVE-2022-0106

Issue 1278960: Security: Heap-use-after-free in autofill::EditAddressProfileView::WindowClosing

Reported by chrom...@gmail.com on Fri, Dec 10, 2021, 6:41 PM EST

Code

VERSION

Chrome Version: 99.0.4759.0 (Developer Build) (x86_64)
Operating System: all

REPRODUCTION CASE

Similar to ~~issue 1240884~~.

1. Run ./chrome --enable-features=AutofillAddressProfileSavePrompt http://localhost:8000/poc.html
2. Click the 'Edit address' icon twice
3. Close the tab

```
==2832==ERROR: AddressSanitizer: heap-use-after-free on address 0x622000393100 at pc 0x0001255885d9 bp 0x7fff5765cdf0 sp 0x7fff5765cde8
READ of size 8 at 0x622000393100 thread T0
    #0 0x1255885d8 in non-virtual thunk to autofill::EditAddressProfileView::WindowClosing() edit_address_profile_view.cc:67
    #1 0x124174274 in views::Widget::OnNativeWidgetDestroying() widget.cc:1409
    #2 0x12421d428 in non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnWindowWillClose() native_widget_mac_ns_window_host.mm:1089
    #3 0x1206ca1a0 in remote_cocoa::NativeWidgetNSWindowBridge::OnWindowWillClose() native_widget_ns_window_bridge.mm:855
    #4 0x1206d814a in -[ViewsNSWindowDelegate windowWillClose:] views_nswindow_delegate.mm:181
    #5 0x7fff84102fbb in __CFNOTIFICATIONCENTER_IS_CALLING_OUT_TO_AN_OBSERVER__+0xb (CoreFoundation:x86_64+0x9afbb)
    #6 0x7fff84102eba in _CFXRegistrationPost+0x1aa (CoreFoundation:x86_64+0x9aeba)
    #7 0x7fff84102c21 in ___CFXNotificationPost_block_invoke+0x31 (CoreFoundation:x86_64+0x9ac21)
    #8 0x7fff840c11b1 in -[_CFXNotificationRegistrar find:object:observer:enumerator:]+0x7e1 (CoreFoundation:x86_64+0x591b1)
    #9 0x7fff840c019a in _CFXNotificationPost+0x29a (CoreFoundation:x86_64+0x5819a)
    #10 0x7fff85b04e86 in -[NSNotificationCenter postNotificationName:object:userInfo:]+0x41 (Foundation:x86_64+0x6e86)
    #11 0x7fff81e77da3 in __18-[NSWindow _close]_block_invoke+0xcc (AppKit:x86_64+0x2ddda3)
    #12 0x7fff81e77c87 in -[NSWindow _close]+0x16c (AppKit:x86_64+0x2ddc87)
    #13 0x1206c11b9 in -[ViewsNSWindowCloseAnimator animationDidEnd:] native_widget_ns_window_bridge.mm:118
    #14 0x7fff8200fe7f in -[NSAnimation _callHandlerWithProgress:didStop:didFinish:]+0x94 (AppKit:x86_64+0x475e7f)
    #15 0x7fff81d1fe32 in -[NSAnimation(NSInternal) _stopAnimation:withDisplayLink:]+0x1e4 (AppKit:x86_64+0x185e32)
    #16 0x7fff81db2c5a in -[NSAnimation(NSInternal) _advanceTimeWithDisplayLink:]+0x133 (AppKit:x86_64+0x218c5a)
    #17 0x7fff81db2a7b in -[NSScreenDisplayLink _fire]+0x148 (AppKit:x86_64+0x218a7b)
    #18 0x7fff840f6873 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_TIMER_CALLBACK_FUNCTION__+0x13 (CoreFoundation:x86_64+0x8e873)
    #19 0x7fff840f6502 in __CFRunLoopDoTimer+0x432 (CoreFoundation:x86_64+0x8e502)
    #20 0x7fff840f6059 in __CFRunLoopDoTimers+0x129 (CoreFoundation:x86_64+0x8e059)
    #21 0x7fff840eda30 in __CFRunLoopRun+0x820 (CoreFoundation:x86_64+0x85a30)
    #22 0x7fff840ecfb3 in CFRunLoopRunSpecific+0x1a3 (CoreFoundation:x86_64+0x84fb3)

    #23 0x7fff8364bebb in RunCurrentEventLoopInMode+0xef (HIToolbox:x86_64+0x30ebb)
    #24 0x7fff8364bcf0 in ReceiveNextEventCommon+0x1af (HIToolbox:x86_64+0x30cf0)
    #25 0x7fff8364bb25 in _BlockUntilNextEventMatchingListInModeWithFilter+0x46 (HIToolbox:x86_64+0x30b25)
```

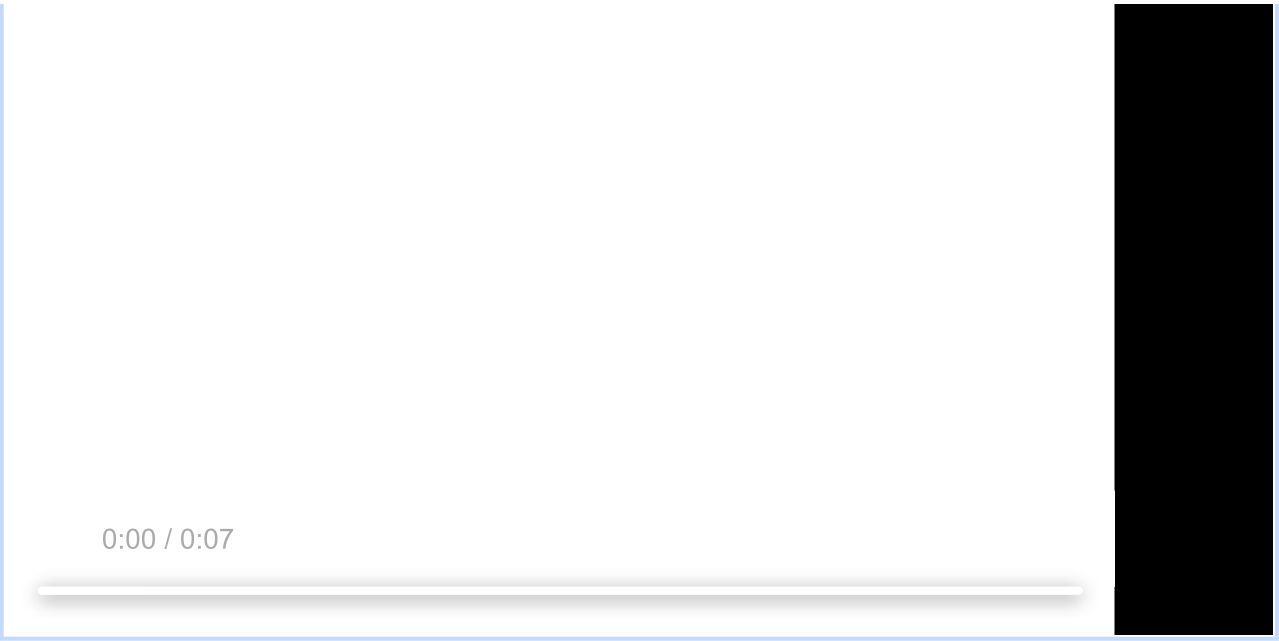
```
   #25 0x7fff8364bb25 in _BlockUntilNextEventMatchingListInModeWithFilter+0x46 (HIToolbox:x86_64+0x30b25)
   #26 0x7fff81be0a03 in _DPSNextEvent+0x45f (AppKit:x86_64+0x46a03)
   #27 0x7fff8235c7ed in -[NSApplication(NSEvent) _nextEventMatchingEventMask:untilDate:inMode:dequeue:]+0xaeb
(AppKit:x86_64+0x7c27ed)
   #28 0x119d7d0c2 in __71-[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke
chrome_browser_application_mac.mm:237
   #29 0x11afea689 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xd471689)
   #30 0x119d7cc6d in -[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]
chrome_browser_application_mac.mm:236
   #31 0x7fff81bd538a in -[NSApplication run]+0x39d (AppKit:x86_64+0x3b38a)
   #32 0x11afff19a in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*)
message_pump_mac.mm:743
   #33 0x11affaf18 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*)
message_pump_mac.mm:161
   #34 0x11af1b7a3 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) thread_controller_with_message_pump_impl.cc:462
   #35 0x11ae567c8 in base::RunLoop::Run(base::Location const&) run_loop.cc:134
   #36 0x1122d36c3 in content::BrowserMainLoop::RunMainMessageLoop() browser_main_loop.cc:989
   #37 0x1122d7b31 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:152
   #38 0x1122cd44c in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:49
   #39 0x119bc4b7a in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool)
content_main_runner_impl.cc:609
   #40 0x119bc3c65 in content::ContentMainRunnerImpl::Run(bool) content_main_runner_impl.cc:972
   #41 0x119bbfad0 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*)
content_main.cc:390
   #42 0x119bc199a in content::ContentMain(content::ContentMainParams const&) content_main.cc:418
   #43 0x10db7db64 in ChromeMain chrome_main.cc:172
   #44 0x10859ebff in main chrome_exe_main_mac.cc:115
   #45 0x7fff99d35234 in start+0x0 (libdyld.dylib:x86_64+0x5234)

0x622000393100 is located 0 bytes inside of 5768-byte region [0x622000393100,0x622000394788)
freed by thread T0 here:
   #0 0x1086f3819  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x47819)
   #1 0x11aed3ca5 in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) unique_ptr.h:54
   #2 0x11aed3c5c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
   #3 0x11aed3c3d in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,

std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1798
    #4 0x11aed3c3d in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1798
    #5 0x11aed3c3d in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1798
    #6 0x11aed3c5c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
    #7 0x11aed3c5c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
    #8 0x11aed3c5c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
    #9 0x11aed3c5c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,

std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
    #10 0x11aed3464 in base::SupportsUserData::~SupportsUserData() __tree:1789
    #11 0x1134de30a in content::WebContentsImpl::~WebContentsImpl() web_contents_impl.cc:1026
```

```
   #11 0x1134dc30a in content::WebContentsImpl::~WebContentsImpl() web_contents_impl.cc:1026
   #12 0x1134deb3d in content::WebContentsImpl::~WebContentsImpl() web_contents_impl.cc:928
   #13 0x124d6221a in TabStripModel::SendDetachWebContentsNotifications(TabStripModel::DetachNotifications*)
unique_ptr.h:54
   #14 0x124d6b1dd in TabStripModel::CloseTabs(base::span<content::WebContents* const, 18446744073709551615ul>,
unsigned int) tab_strip_model.cc:1798
   #15 0x124d6c803 in TabStripModel::CloseWebContentsAt(int, unsigned int) tab_strip_model.cc:767
   #16 0x125b055a8 in BrowserTabStripController::CloseTab(int) browser_tab_strip_controller.cc:372
   #17 0x125bc7bf6 in TabStrip::CloseTabInternal(int, CloseTabSource) tab_strip.cc:3067
   #18 0x125bc7514 in TabStrip::CloseTab(Tab*, CloseTabSource) tab_strip.cc:1981
   #19 0x125b19663 in Tab::CloseButtonPressed(ui::Event const&) tab.cc:1073
   #20 0x123fac20b in views::Button::DefaultButtonControllerDelegate::NotifyClick(ui::Event const&) button.cc:66
   #21 0x123fbf2ca in views::ButtonController::OnMouseReleased(ui::MouseEvent const&) button_controller.cc
   #22 0x123f9c7e6 in ui::ScopedTargetHandler::OnEvent(ui::Event*) scoped_target_handler.cc:28
   #23 0x11d20737f in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:191
   #24 0x11d206c20 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:84
   #25 0x124158aa7 in views::internal::RootView::OnMouseReleased(ui::MouseEvent const&) root_view.cc:480
   #26 0x124177f48 in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1549
   #27 0x124219bac in non-virtual thunk to
views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event>
>) native_widget_mac_ns_window_host.mm:854
   #28 0x1206b28f9 in -[BridgedContentView mouseEvent:] bridged_content_view.mm:595
   #29 0x11bbaefe9 in -[BaseView mouseUp:] base_view.mm:128

previously allocated by thread T0 here:
   #0 0x1086f36d0  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x476d0)
   #1 0x10db7b4e7 in operator new(unsigned long) new.cpp:67
   #2 0x1252c389e in autofill::SaveUpdateAddressProfileBubbleControllerImpl::OnEditButtonClicked()
save_update_address_profile_bubble_controller_impl.cc:99
   #3 0x123fbaf59 in
base::internal::Invoker<base::internal::BindState<views::Button::PressedCallback::PressedCallback(base::RepeatingCallbac
k<void ()>)::$_0, base::RepeatingCallback<void ()> >, void (ui::Event const&)>::Run(base::internal::BindStateBase*,
ui::Event const&) callback.h:167
   #4 0x123fac20b in views::Button::DefaultButtonControllerDelegate::NotifyClick(ui::Event const&) button.cc:66
   #5 0x123fbf2ca in views::ButtonController::OnMouseReleased(ui::MouseEvent const&) button_controller.cc
   #6 0x123f9c7e6 in ui::ScopedTargetHandler::OnEvent(ui::Event*) scoped_target_handler.cc:28
   #7 0x11d20737f in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:191
   #8 0x11d206c20 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:84
   #9 0x124158aa7 in views::internal::RootView::OnMouseReleased(ui::MouseEvent const&) root_view.cc:480
   #10 0x124177f48 in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1549
   #11 0x124219bac in non-virtual thunk to
views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event>
>) native_widget_mac_ns_window_host.mm:854
   #12 0x1206b28f9 in -[BridgedContentView mouseEvent:] bridged_content_view.mm:595
   #13 0x11bbaefe9 in -[BaseView mouseUp:] base_view.mm:128
   #14 0x7fff824d68dd in -[NSWindow(NSEventRouting) _reallySendEvent:isDelayedEvent:]+0x607
(AppKit:x86_64+0x93c8dd)
   #15 0x7fff824d5f09 in -[NSWindow(NSEventRouting) sendEvent:]+0x21c (AppKit:x86_64+0x93bf09)
   #16 0x1206bdf5d in -[NativeWidgetMacNSWindow sendEvent:] native_widget_mac_nswindow.mm:298
   #17 0x7fff8235a680 in -[NSApplication(NSEvent) sendEvent:]+0x478 (AppKit:x86_64+0x7c0680)
   #18 0x119d7fad4 in __34-[BrowserCrApplication sendEvent:]_block_invoke chrome_browser_application_mac.mm:335

   #19 0x11afea689 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xd471689)
   #20 0x119d7ee4e in -[BrowserCrApplication sendEvent:] chrome_browser_application_mac.mm:319
   #21 0x7fff81bd53d6 in -[NSApplication run]+0x3c9 (AppKit:x86_64+0x2b3d6)
```

```
    #21 0x7fff81bd53d6 in -[NSApplication run]+0x3e9 (AppKit:x86_64+0x3b3d6)
    #22 0x11afff19a in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*)
message_pump_mac.mm:743
    #23 0x11affaf18 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*)
message_pump_mac.mm:161
    #24 0x11af1b7a3 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) thread_controller_with_message_pump_impl.cc:462
    #25 0x11ae567c8 in base::RunLoop::Run(base::Location const&) run_loop.cc:134
    #26 0x1122d36c3 in content::BrowserMainLoop::RunMainMessageLoop() browser_main_loop.cc:989
    #27 0x1122d7b31 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:152
    #28 0x1122cd44c in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:49
    #29 0x119bc4b7a in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool)
content_main_runner_impl.cc:609

SUMMARY: AddressSanitizer: heap-use-after-free edit_address_profile_view.cc:67 in non-virtual thunk to
autofill::EditAddressProfileView::WindowClosing()
Shadow bytes around the buggy address:
  0x1c44000725d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c44000725e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c44000725f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c4400072600: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c4400072610: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x1c4400072620:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c4400072630: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c4400072640: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c4400072650: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c4400072660: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c4400072670: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
```

screen.mov
12.1 MB View Download

[redacted]



poc.html
1.2 KB View Download

Comment 1 by satishy@chromium.org on Sun, Dec 12, 2021, 10:07 PM EST Project Member

Labels: Needs-Triage-M99
Components: UI>Browser>Autofill

Comment 2 by kavvaru@chromium.org on Mon, Dec 13, 2021, 4:43 AM EST Project Member

Cc: mamir@chromium.org kavvaru@chromium.org
Labels: Triaged-ET

ccing the dev mamir@ from the ~~issue 1240884~~ to get more inputs from dev team.

Thanks,

Comment 3 by koerber@google.com on Thu, Dec 16, 2021, 5:40 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: mamir@chromium.org

Comment 4 by battre@chromium.org on Thu, Dec 16, 2021, 9:24 AM EST Project Member

Cc: koerber@google.com
Labels: Restrict-View-SecurityTeam Security_Needs_Attention-Severity

Comment 5 by mamir@chromium.org on Thu, Dec 16, 2021, 9:27 AM EST Project Member

Cc: battre@chromium.org

Comment 6 by battre@chromium.org on Thu, Dec 16, 2021, 9:27 AM EST Project Member

Labels: M-96

Comment 7 by mamir@chromium.org on Thu, Dec 16, 2021, 9:45 AM EST Project Member

I am not able to repro this on 99.0.4766.0

How is it possible to hit the Edit button twice?
The screencast shows the Edit Prompt visible while the Edit dialog is open.

This shouldn't be the case.

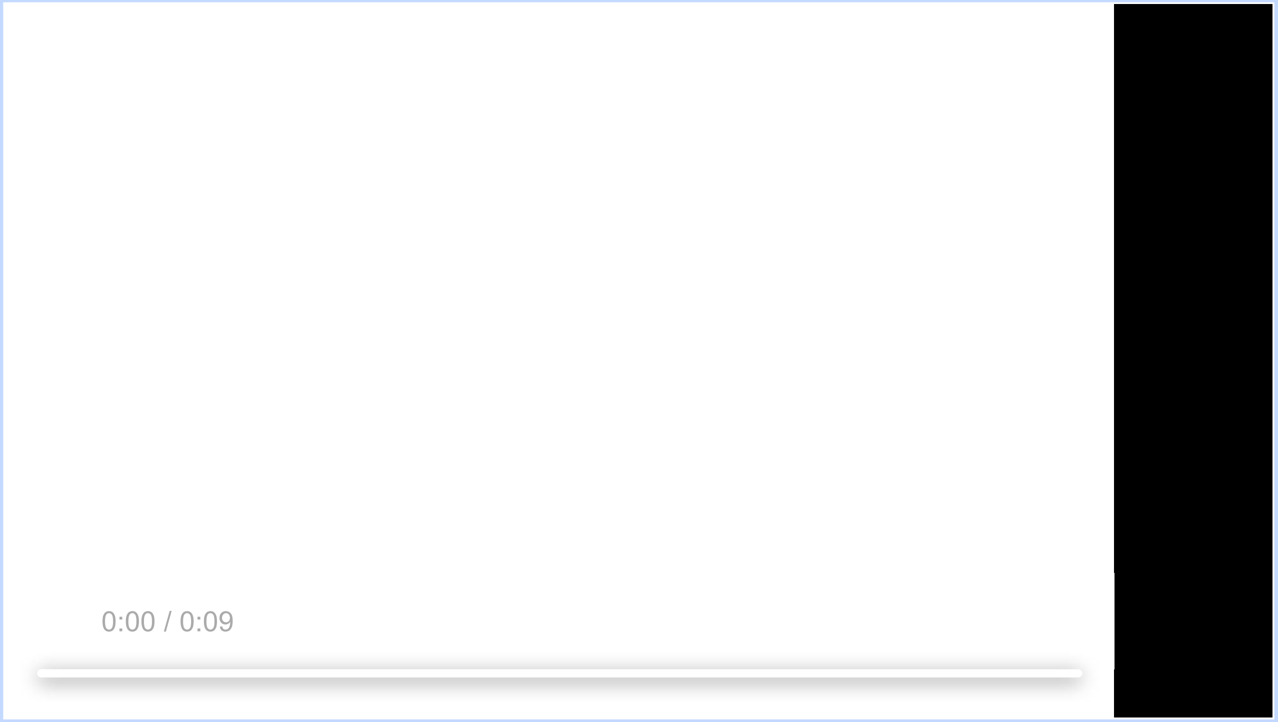
@reporter: Could you please clarify if this indeed the case?

Comment 8 by chrom...@gmail.com on Thu, Dec 16, 2021, 11:36 AM EST

Can you please try to repro the crash with this PoC.

p1.html
1.3 KB View Download

Screencast from 16 17:34:24 01+ 2021 ,دجنبر.webm
1.3 MB View Download



Comment 9 by mamir@chromium.org on Thu, Dec 16, 2021, 1:20 PM EST Project Member

Cc: schwering@google.com

Comment 10 by Git Watcher on Thu, Dec 16, 2021, 3:46 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a465e42d95183ea523e7d7190a40224dcc818a86

commit a465e42d95183ea523e7d7190a40224dcc818a86
Author: Mohamed Amir Yosef <mamir@chromium.org>

Date: Thu Dec 16 20:45:47 2021

[Autofill] Allow only one EditAddressDialogview

[Autofill] Allow only one EditAddressDialogView

Since we have only one controller per tab, it makes sense to allow only
one EditAddressDialogView as well.

~~Bug: 1278960~~
Change-Id: I8970ba453c6404e346372c68429544e38e5960b3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3344636
Reviewed-by: Christoph Schwering <schwering@google.com>
Commit-Queue: Christoph Schwering <schwering@google.com>
Cr-Commit-Position: refs/heads/main@{#952499}

[modify]
https://crrev.com/a465e42d95183ea523e7d7190a40224dcc818a86/chrome/browser/ui/autofill/edit_address_profile_dialog_controller_impl.cc

Comment 11 by mamir@chromium.org on Thu, Dec 16, 2021, 3:54 PM EST Project Member

Status: Fixed (was: Assigned)
Labels: -Security_Needs_Attention-Severity Security_Severity-High OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1

It's a UAF bug that is in code behind a Finch flag but that enabled already for 20% on Stable.

Comment 12 by sheriffbot on Fri, Dec 17, 2021, 1:39 PM EST Project Member

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

Comment 13 by mamir@chromium.org on Mon, Dec 20, 2021, 3:57 AM EST Project Member

Labels: Build Merge-Request-98 Merge-Request-97

Comment 14 by sheriffbot on Mon, Dec 20, 2021, 4:01 AM EST Project Member

Labels: -Merge-Request-98 Hotlist-Merge-Approved Merge-Approved-98

Merge approved: your change passed merge requirements and is auto-approved for M98. Please go ahead and merge the CL to branch 4758 (refs/branch-heads/4758) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: govind (Android), harrysouders (iOS), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 15 by sheriffbot on Mon, Dec 20, 2021, 4:01 AM EST Project Member

Labels: -Merge-Request-97 Hotlist-Merge-Review Merge-Review-97

Merge review required: M97 has already been cut for stable release.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents

https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

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

Comment 16 by mamir@chromium.org on Mon, Dec 20, 2021, 4:16 AM EST Project Member

1- Yes, it's a UAF bug that is already hitting 20% of Stable users.

2- https://crrev.com/c/3344636

3- Yes!

4- It's a feature that's being rollout it, and it's hitting 20% of Stable users now.
It's behind a feature flag, however disabling it, will produce suboptimal user experience.
In addition, the repro steps require non-standard complex behavior
- have some background code to submit address forms without user intervention
- the user has to click the Edit button on one address save prompts.
- Another address save prompt appears while the first Edit prompt is still visible.
- The user has to click the Edit button while the first Edit address prompt is still open.
Given how involved the repro steps, merging the fix is more plausible than taking down the rollout!

6- It doesn't require manual verification! The fix has been verified manually already by the CL reviewer!

Comment 17 by Git Watcher on Mon, Dec 20, 2021, 5:29 AM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/40edf82fdf87b74dca867ea668ef64a7c4d28b13

commit 40edf82fdf87b74dca867ea668ef64a7c4d28b13
Author: Mohamed Amir Yosef <mamir@chromium.org>
Date: Mon Dec 20 10:28:23 2021

[Autofill] Allow only one EditAddressDialogview

Since we have only one controller per tab, it makes sense to allow only
one EditAddressDialogView as well.

(cherry picked from commit a465e42d95183ea523e7d7190a40224dcc818a86)

~~Bug: 1278960~~
Change-Id: I8970ba453c6404e346372c68429544e38e5960b3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3344636
Reviewed-by: Christoph Schwering <schwering@google.com>
Commit-Queue: Christoph Schwering <schwering@google.com>
Cr-Original-Commit-Position: refs/heads/main@{#952499}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347574
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Auto-Submit: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Matthias Körber <koerber@google.com>

Reviewed-by: Matthias Körber <koerber@google.com>
Commit-Queue: Matthias Körber <koerber@google.com>
Cr-Commit-Position: refs/branch-heads/4758@{#121}
Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify]
https://crrev.com/40edf82fdf87b74dca867ea668ef64a7c4d28b13/chrome/browser/ui/autofill/edit_address_profile_dialog_controller_impl.cc

Comment 18 by pbommana@google.com on Tue, Dec 21, 2021, 10:57 PM EST Project Member

Cc: adetaylor@chromium.org amyressler@chromium.org

Based on the labels Security_Severity-High assuming that this is Security issue hence cc'ing Adetaylor@ and Amyressler@ Security TPM's for Merge decision.

Note : We have already cut M97 Stable RC which is scheduled to get rolled out to Stable on Jan-04th-2022.

Comment 19 by battre@chromium.org on Wed, Dec 22, 2021, 7:29 AM EST Project Member

Here is the situation:

If the user submits an address, we will show a save dialog (currently rolled out to 20% stable to M94+). On Desktop that dialog has an edit button and if you *double* click (instead of single click) that button, we have a use after free. My non-security-expert impression would be that this is hard to exploit, but intuition is often wrong in security cases.

I would expect that the problem is triggered very rarely. Our metrics indicate that very few users press the edit button.
https://uma.googleplex.com/p/chrome/histograms?sid=384fc6ccbe2b73fc44bc5c415551b978

Given that the dialog is pretty visible and already rolled out to 20%, the question is whether we have to roll back or fix forward.

How would you feel about merging the fix to M97 for the first respin and once this is released, disable the feature on all previous versions?

Comment 20 by mamir@chromium.org on Wed, Dec 22, 2021, 7:38 AM EST Project Member

I just would like to clarify one thing.
Here are the steps to exploit this bug:

- If the user submits an address, we will show a save dialog.
- On Desktop that dialog has an edit button.
- The user has to click the Edit dialog which open a modal dialog.
- Another form submission needs to happen while the dialog is open (e.g. by some JavaScript).
- Another Save dialog is open with an Edit button.
- The user has to click the second Edit button (while the first is still open).
- User-after-free happens when closing the tab.

Comment 21 by amyressler@chromium.org on Mon, Dec 27, 2021, 5:00 PM EST Project Member

Labels: Type-Bug-Security

moving back to bug-security so this issue ends up in the correct security queues

Comment 22 by sheriffbot on Mon, Dec 27, 2021, 5:02 PM EST Project Member

Labels: external_security_report

Comment 23 by sheriffbot on Mon, Dec 27, 2021, 5:02 PM EST Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We’ve reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 24 by amyressler@chromium.org on Mon, Dec 27, 2021, 5:07 PM EST Project Member

Thanks for the question and insight in comments #19 and 20. Given this is an issue that results in browser process memory corruption, I'm not wild about letting it sit, but given this requires a fair amount user gesture (in terms of double/second clicks) as well as tab closure to trigger, I'm okay with not merging this back to M96, but the feature should be disabled on M96 as it will be Extended channel as M97 is stable.
Please go ahead and merge to M97, branch 4758 as soon as possible. Thanks!

Comment 25 by amyressler@chromium.org on Mon, Dec 27, 2021, 5:08 PM EST Project Member

Status: Fixed (was: Assigned)
Labels: FoundIn-96

Comment 26 by sheriffbot on Mon, Dec 27, 2021, 5:08 PM EST Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We’ve reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 27 by sheriffbot on Mon, Dec 27, 2021, 5:08 PM EST Project Member

Labels: Security_Impact-Extended

Comment 28 by amyressler@chromium.org on Mon, Dec 27, 2021, 5:09 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 29 by mamir@chromium.org on Tue, Dec 28, 2021, 12:03 PM EST Project Member

Thank you amyressler@ for looking into this and your insightis!
I have 2 questions, please:

- Regarding "Please go ahead and merge to M97, branch 4758 as soon as possible. "
IIUC, M97 is branched at 4692.
Could you please confirm my understanding?

- Do I need the "Merge-Approved-97" label before I can merge my the CL?

Thank you!

Comment 30 by amyressler@chromium.org on Tue, Dec 28, 2021, 12:41 PM EST Project Member

Labels: -Merge-Review-97 Merge-Approved-97

Hi mamir@, thanks for your questions, but my sincere apologies for all my errors that made them necessary.
You are correct, M97 is branch 4692; this was on the heels of doing reviews for M98 merge.
And I forgot to add the merge-approved label for that, thus adding for greater confusion. :)
It's now added! Thanks!!

Comment 31 by sheriffbot on Tue, Dec 28, 2021, 12:41 PM EST Project Member

Labels: reward-topanel

Comment 32 by mamir@chromium.org on Tue, Dec 28, 2021, 12:50 PM EST Project Member

Thank you Amy for clarification.
I have prepared https://crrev.com/c/3359419 for the merge!
Looking for a reviewer to rslgtm it at the moment!

Comment 33 by Git Watcher on Tue, Dec 28, 2021, 1:56 PM EST Project Member

Labels: -merge-approved-97 merge-merged-4692 merge-merged-97

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e89aed2a562e2cdf797fe6e4ed4f35e2cfb05215

commit e89aed2a562e2cdf797fe6e4ed4f35e2cfb05215
Author: Mohamed Amir Yosef <mamir@chromium.org>
Date: Tue Dec 28 18:55:39 2021

[Autofill] Allow only one EditAddressDialogview

Since we have only one controller per tab, it makes sense to allow only
one EditAddressDialogView as well.

(cherry picked from commit a465e42d95183ea523e7d7190a40224dcc818a86)

~~Bug: 1278960~~
Change-Id: I8970ba453c6404e346372c68429544e38e5960b3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3344636
Reviewed-by: Christoph Schwering <schwering@google.com>
Commit-Queue: Christoph Schwering <schwering@google.com>
Cr-Original-Commit-Position: refs/heads/main@{#952499}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3359419
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Auto-Submit: Mohamed Amir Yosef <mamir@chromium.org>
Reviewed-by: Vasilii Sukhanov <vasilii@chromium.org>
Commit-Queue: Vasilii Sukhanov <vasilii@chromium.org>

Commit-Queue: Vasilii Sukhanov <vasilii@chromium.org>
Cr-Commit-Position: refs/branch-heads/4692@{#1237}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify]
https://crrev.com/e89aed2a562e2cdf797fe6e4ed4f35e2cfb05215/chrome/browser/ui/autofill/edit_address_profile_dialog_controller_impl.cc

Comment 34 by amyressler@chromium.org on Tue, Jan 4, 2022, 11:50 AM EST Project Member

Labels: Release-0-M97

Comment 35 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0106 CVE_description-missing

Comment 36 by gmpritchard@google.com on Wed, Jan 5, 2022, 12:09 PM EST Project Member

Labels: LTS-Merge-Candidate

Comment 37 by gmpritchard@google.com on Wed, Jan 12, 2022, 4:38 PM EST Project Member

Labels: -LTS-Merge-Candidate

Removing LTS label since the feature is disabled in M96.

Comment 38 by gmpritchard@google.com on Thu, Jan 13, 2022, 12:09 PM EST Project Member

Labels: LTS-NotApplicable-96

Comment 39 by amyressler@google.com on Thu, Jan 13, 2022, 6:03 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-7000

*** 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 40 by amyressler@chromium.org on Thu, Jan 13, 2022, 6:18 PM EST Project Member

Congratulations, Khalil! The VRP Panel has decided to award you $7,000 for this report. Thank you for your efforts and nice work!

Comment 41 by amyressler@google.com on Fri, Jan 14, 2022, 5:32 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 42 by sheriffbot on Tue, Apr 5, 2022, 1:29 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

Comment 43 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted