Starred by 4 users

Owner:	pbos@chromium.org
CC:	voit@google.com corising@chromium.org collinbaker@chromium.org sky@chromium.org
Status:	Verified *(Closed)*
Components:	UI>Browser>Bookmarks
Modified:	Oct 29, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
reward-20000
CVE_description-submitted
M-91
Target-91
external_security_report
Target-93
merge-merged-4430
merge-merged-90
FoundIn-91
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
merge-merged-4577
merge-merged-93
LTS-Size-Small
LTS-Complexity-Minimal
Release-1-M92

Issue 1227777: Security: HeapOverflow in RecentlyUsedFoldersComboModel

Reported by leecraso@gmail.com on Fri, Jul 9, 2021, 2:10 PM EDT

Code

VULNERABILITY DETAILS

The size of |item_|[1] could be reduced after the tab is bookmarked into the default folder but before painting the RecentlyUsedFoldersComboView. |selected_index_|[2] can be equal to the size of |item_|, then the out of bounds will be triggered when GetItemAt is called[3].

[1]. https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/bookmarks/recently_used_folders_combo_model.h;l=84;drc=8324b2da4aa6ce3c38ead55ff1f3c2844c21a0e5
[2]. https://source.chromium.org/chromium/chromium/src/+/main:ui/views/controls/combobox/combobox.cc;l=615;drc=8324b2da4aa6ce3c38ead55ff1f3c2844c21a0e5
[3]. https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc;l=105;drc=3f97e29466e8450418d0897f21706ffc0d1aef20

VERSION

Chrome Version: stable
Operating System: Linux, ChromeOS, Win, Mac

REPRODUCTION CASE

Install the extension and bookmark any tab.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: browser
Crash State: see asan file

CREDIT INFORMATION

Reporter credit: Leecraso and Guang Gong of 360 Alpha Lab

asan
12.4 KB View Download

manifest.json
172 bytes View Download

poc.js
845 bytes View Download

Demo.mp4
599 KB View Download

Comment 1 by sheriffbot on Fri, Jul 9, 2021, 2:15 PM EDT Project Member

Labels: external_security_report

Comment 2 by rsesek@chromium.org on Fri, Jul 9, 2021, 4:34 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: pbos@chromium.org
Cc: corising@chromium.org collinbaker@chromium.org
Labels: FoundIn-91 Security_Severity-High OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2
Components: UI>Browser>Bookmarks

Thanks, confirmed on macOS.

pbos: Can you please look or find a better top-chrome owner?

Comment 3 by sheriffbot on Fri, Jul 9, 2021, 4:38 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 4 by rsesek@chromium.org on Fri, Jul 9, 2021, 6:24 PM EDT Project Member

With speculative patch:

==1721==ERROR: AddressSanitizer: container-overflow on address 0x60c000372388 at pc 0x00011c966aeb bp 0x7ffeefbfc670 sp 0x7ffeefbfc668
READ of size 4 at 0x60c000372388 thread T0

Process 1721 stopped
* thread #1, name = 'CrBrowserMain', queue = 'com.apple.main-thread', stop reason = signal SIGSTOP
    frame #0: 0x00007fff69aa081e libsystem_kernel.dylib`read + 10
libsystem_kernel.dylib`read:
-> 0x7fff69aa081e <+10>: jae   0x7fff69aa0828   ; <+20>
    0x7fff69aa0820 <+12>: mov   rdi, rax
    0x7fff69aa0823 <+15>: jmp   0x7fff69aa122d   ; cerror
    0x7fff69aa0828 <+20>: ret
Target 0: (Chromium) stopped.
(lldb) bt
* thread #1, name = 'CrBrowserMain', queue = 'com.apple.main-thread', stop reason = signal SIGSTOP
  * frame #0: 0x00007fff69aa081e libsystem_kernel.dylib`read + 10
    frame #1: 0x000000010031c235 libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol918$$libclang_rt.asan_osx_dynamic.dylib + 21
    frame #2: 0x00000001003270dd libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1195$$libclang_rt.asan_osx_dynamic.dylib + 61
    frame #3: 0x0000000100326dd9 libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1189$$libclang_rt.asan_osx_dynamic.dylib + 233
    frame #4: 0x000000010032762d libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1206$$libclang_rt.asan_osx_dynamic.dylib + 93
    frame #5: 0x0000000100325c9a libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1171$$libclang_rt.asan_osx_dynamic.dylib + 138
    frame #6: 0x000000010032435a libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1125$$libclang_rt.asan_osx_dynamic.dylib + 42
    frame #7: 0x000000010032427c libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1124$$libclang_rt.asan_osx_dynamic.dylib + 236
    frame #8: 0x00000001003245ee libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol1127$$libclang_rt.asan_osx_dynamic.dylib + 126
    frame #9: 0x00000001002c9b7c libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol168$$libclang_rt.asan_osx_dynamic.dylib + 412
    frame #10: 0x000000010030793b libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol583$$libclang_rt.asan_osx_dynamic.dylib + 59
    frame #11: 0x000000010030737a libclang_rt.asan_osx_dynamic.dylib`___lldb_unnamed_symbol580$$libclang_rt.asan_osx_dynamic.dylib + 1466
    frame #12: 0x00000001003307ee8 libclang_rt.asan_osx_dynamic.dylib`__asan_report_load4 + 40
    frame #13: 0x000000011c966aeb Chromium Framework`RecentlyUsedFoldersComboModel::MaybeChangeParent(this=<unavailable>, node=<unavailable>, selected_index=4) at recently_used_folders_combo_model.cc:225:30 [opt]
    frame #14: 0x000000011d14fe97 Chromium Framework`BookmarkBubbleView::BookmarkBubbleDelegate::ApplyEdits(this=<unavailable>) at bookmark_bubble_view.cc:134:23 [opt]
    frame #15: 0x000000011237b84d Chromium Framework`ui::DialogModel::OnDialogAccepted(base::PassKey<ui::DialogModelHost>) [inlined] base::OnceCallback<void ()>::Run() && at callback.h:98:12 [opt]
    frame #16: 0x000000011237b7fc Chromium Framework`ui::DialogModel::OnDialogAccepted(this=<unavailable>, (null)=<unavailable>) at dialog_model.cc:141 [opt]
    frame #17: 0x000000011c28d9e2 Chromium Framework`views::DialogDelegate::Accept() [inlined] base::OnceCallback<void ()>::Run(this=0x00007ffeefbfc9e0) && at callback.h:98:12 [opt]
    frame #18: 0x000000011c28d98a Chromium Framework`views::DialogDelegate::Accept() [inlined] views::DialogDelegate::RunCloseCallback(this=<unavailable>, callback=base::OnceClosure @ 0x00007ffeefbfc9e0)>) at dialog_delegate.cc:178 [opt]
    frame #19: 0x000000011c28d967 Chromium Framework`views::DialogDelegate::Accept(this=<unavailable>) at dialog_delegate.cc:171 [opt]
    frame #20: 0x000000011c290425 Chromium Framework`views::DialogDelegate::AcceptDialog(this=0x000061b0000ff880) at dialog_delegate.cc:400:34 [opt]
    frame #21: 0x000000011c28a72f Chromium Framework`views::DialogClientView::ButtonPressed(this=<unavailable>, type=DIALOG_BUTTON_OK, event=0x00007ffeefbfd220) at dialog_client_view.cc:286:48 [opt]
    frame #22: 0x000000011bf4d62c Chromium Framework`views::Button::DefaultButtonControllerDelegate::NotifyClick(this=<unavailable>, event=<unavailable>) at button.cc:66:13 [opt]
    frame #23: 0x000000011bf60a29 Chromium Framework`views::ButtonController::OnMouseReleased(this=0x0000603000645400, event=<unavailable>) at button_controller.cc:0:34 [opt]
    frame #24: 0x0000000113ba2cd5 Chromium Framework`ui::ScopedTargetHandler::OnEvent(this=0x00006070005d21b0, event=<unavailable>) at scoped_target_handler.cc:28:24 [opt]
    frame #25: 0x0000000113b94b80 Chromium Framework`ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) [inlined] ui::EventDispatcher::DispatchEvent(this=0x00007ffeefbfd0c0, handler=0x00006070005d21b0, event=0x00007ffeefbfd220) at event_dispatcher.cc:191:12 [opt]
    frame #26: 0x0000000113b94af2 Chromium Framework`ui::EventDispatcher::ProcessEvent(this=<unavailable>, target=0x000061a0001a8280, event=<unavailable>) at event_dispatcher.cc:140 [opt]
    frame #27: 0x0000000113b94413 Chromium Framework`ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) [inlined] ui::EventDispatcherDelegate::DispatchEventToTarget(this=0x00006180001f8480, target=0x000061a0001a8280, event=0x00007ffeefbfd220) at event_dispatcher.cc:84:14 [opt]
    frame #28: 0x0000000113b94364 Chromium Framework`ui::EventDispatcherDelegate::DispatchEvent(this=<unavailable>, target=0x000061a0001a8280, event=<unavailable>) at event_dispatcher.cc:56 [opt]
    frame #29: 0x000000011c248a4b Chromium Framework`views::internal::RootView::OnMouseReleased(this=0x00006180001f8480, event=0x0000611000906040) at

root_view.cc:480:9 [opt]
    frame #30: 0x000000011c2653b8 Chromium Framework`views::Widget::OnMouseEvent(this=<unavailable>, event=<unavailable>) at widget.cc:1463:20 [opt]
    frame #31: 0x000000011c2ad4ed Chromium Framework`non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event> >) [inlined] views::NativeWidgetMacNSWindowHost::OnMouseEvent(this=<unavailable>, event=nullptr) at native_widget_mac_ns_window_host.mm:846:28 [opt]
    frame #32: 0x000000011c2ad43a Chromium Framework`non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event> >) at native_widget_mac_ns_window_host.mm:0 [opt]
    frame #33: 0x00000001184fd30c Chromium Framework`-[BridgedContentView mouseEvent:](self=<unavailable>, _cmd=<unavailable>, theEvent=0x0000611000906180) at bridged_content_view.mm:595:20 [opt]
    frame #34: 0x000000011184fa7ae Chromium Framework`-[BridgedContentView processCapturedMouseEvent:](self=<unavailable>, _cmd=<unavailable>, theEvent=0x0000611000906180) at bridged_content_view.mm:308:7 [opt]
    frame #35: 0x0000000118507f7c Chromium Framework`invocation function for block in remote_cocoa::CocoaMouseCapture::ActiveEventTap::Init(.block_descriptor=<unavailable>, event=0x0000611000906180) at mouse_capture.mm:91:25 [opt]
    frame #36: 0x00007fff2cc6f982 AppKit`_NSSendEventToObservers + 323
    frame #37: 0x00007fff2cc6e446 AppKit`-[NSApplication(NSEvent) sendEvent:] + 82

Comment 5 by rsesek@chromium.org on Fri, Jul 9, 2021, 6:24 PM EDT Project Member

Patch: https://chromium-review.googlesource.com/c/chromium/src/+/3018568/3

Comment 6 by pbos@chromium.org on Fri, Jul 9, 2021, 6:30 PM EDT Project Member

Looks like we have more than one problem and it may be worth looking at the root cause instead of duct taping. :(

.. which is actually good.

Comment 7 by sheriffbot on Sat, Jul 10, 2021, 12:46 PM EDT Project Member

Labels: M-91 Target-91

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 8 by sheriffbot on Sat, Jul 10, 2021, 1:26 PM EDT Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity High. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 9 by leecraso@gmail.com on Mon, Jul 12, 2021, 4:40 AM EDT

yes, it's not a unique case. The problem is that the selected_index and the size of items_ are not synchronized. Such as another case[1]:

Also install this extension and bookmark any tab.

[1].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc;l=225;drc=3f97e29466e8450418d0897f21706ffc0d1aef20

asan2
13.1 KB View Download

manifest.json
173 bytes View Download

poc2.js
1019 bytes View Download

Comment 10 by leecraso@gmail.com on Wed, Jul 21, 2021, 8:43 AM EDT

Hi, friendly ping.

Comment 11 by pbos@chromium.org on Wed, Jul 21, 2021, 7:42 PM EDT Project Member

Sorry about the slow response I've been juggling a few other things and was just out of office for a few days. I've got an idea for rsesek@'s issue in #4 and hope to get something up by today or tomorrow.

Comment 12 by pbos@chromium.org on Thu, Jul 22, 2021, 1:24 PM EDT Project Member

Cc: sky@chromium.org

+cc sky@ for reviewer visibility into bug

Comment 13 by Git Watcher on Thu, Jul 22, 2021, 8:02 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d2e1d6871cf7ca9dbbc82a400be49234d20f98cf

commit d2e1d6871cf7ca9dbbc82a400be49234d20f98cf
Author: Peter Boström <pbos@chromium.org>
Date: Fri Jul 23 00:01:38 2021

Fix RecentlyUsedFoldersComboModel heap overflows

This fixes a few bugs:
* RecentlyUsedFoldersComboModel::RemoveNode() would not inform its
  observers of changes.
* RecentlyUsedFoldersComboModel::GetDefaultIndex() did not behave well
  after model changes (could end up using a cached out-of-bounds index).
* BubbleDialogModelHost would not pass on selected-index updates unless
  the user changed the index by performing a combobox action (not true
  when an Extension removes a bookmark folder).

This also replaces off-by-one index correction changes with CHECKs for
index correctness inside views::Combobox. This turns security bugs into
crash bugs and also is likelier to get us better crash stacks if this
happens in the wild as well.

~~Bug: 1227777~~
Change-Id: I9b851129fee4bdd249c1db77b01312b6671784be
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018568
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Peter Boström <pbos@chromium.org>
Cr-Commit-Position: refs/heads/master@{#904551}

[modify] https://crrev.com/d2e1d6871cf7ca9dbbc82a400be49234d20f98cf/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc
[modify] https://crrev.com/d2e1d6871cf7ca9dbbc82a400be49234d20f98cf/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.h

[modify] https://crrev.com/d2e1d6871cf7ca9dbbc82a400be49234d20f98cf/ui/views/bubble/bubble_dialog_model_host.cc
[modify] https://crrev.com/d2e1d6871cf7ca9dbbc82a400be49234d20f98cf/ui/views/controls/combobox/combobox.cc
[modify] https://crrev.com/d2e1d6871cf7ca9dbbc82a400be49234d20f98cf/ui/views/controls/combobox/combobox.h

Comment 14 by pbos@chromium.org on Thu, Jul 22, 2021, 8:14 PM EDT Project Member

Status: Fixed (was: Assigned)

This CL description is outdated, but the bug should be fixed. I ran asan builds and found both of your bugs + a third, that are all resolved at least locally for me. Please verify if you would. :)

Comment 15 by sheriffbot on Fri, Jul 23, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 16 by sheriffbot on Fri, Jul 23, 2021, 1:43 PM EDT Project Member

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

Comment 17 by rsesek@chromium.org on Fri, Jul 23, 2021, 4:17 PM EDT Project Member

Verified locally using an ASan build at 57bb5b3e3044c828e3f4f87df90d1731ab9503c5

Comment 18 by rsesek@chromium.org on Fri, Jul 23, 2021, 4:18 PM EDT Project Member

Status: Verified (was: Fixed)

Comment 19 by pbos@chromium.org on Fri, Jul 23, 2021, 7:47 PM EDT Project Member

Labels: Merge-Request-93 Merge-Request-94

Comment 20 by pbommana@google.com on Sat, Jul 24, 2021, 9:30 AM EDT Project Member

Labels: Target-93

Comment 21 by adetaylor@google.com on Sat, Jul 24, 2021, 11:44 AM EDT Project Member

Labels: -Merge-Request-94 Merge-Request-92 Merge-Request-91

Adding the merge requests which Sheriffbot would normally have added.

Comment 22 by sheriffbot on Sat, Jul 24, 2021, 11:48 AM EDT Project Member

Labels: -Merge-Request-92 Merge-Review-92 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/+/main/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), benmason@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 23 by sheriffbot on Sat, Jul 24, 2021, 7:50 PM EDT Project Member

Labels: -Merge-Request-93 Hotlist-Merge-Approved Merge-Approved-93

Your change meets the bar and is auto-approved for M93. Please go ahead and merge the CL to branch 4577 (refs/branch-heads/4577) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: benmason@(Android), govind@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 24 by pbommana@google.com on Sun, Jul 25, 2021, 9:15 AM EDT Project Member

Your change has been approved for M93. Please go ahead and merge the CL to branch 4577 manually asap so that it would be part of this week's Dev/Beta release.

Comment 25 by pbos@chromium.org on Mon, Jul 26, 2021, 1:03 PM EDT Project Member

Re #22:
1. Yes, remote heap overflow.
2. crrev.com/c/3018568
3. Yes, see #17
4. M92/M93 covers stable/beta.
5. Remote heap overflow, security bug.
6. No
7. N/A

Comment 26 by Git Watcher on Mon, Jul 26, 2021, 2:35 PM EDT Project Member

Labels: -merge-approved-93 merge-merged-4577 merge-merged-93

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/cb19602196e186a7d2ee5525ddb5d63a416fe9fd

commit cb19602196e186a7d2ee5525ddb5d63a416fe9fd
Author: Peter Boström <pbos@chromium.org>
Date: Mon Jul 26 18:34:57 2021

Fix RecentlyUsedFoldersComboModel heap overflows

This fixes a few bugs:
* RecentlyUsedFoldersComboModel::RemoveNode() would not inform its
observers of changes.
* RecentlyUsedFoldersComboModel::GetDefaultIndex() did not behave well
after model changes (could end up using a cached out-of-bounds index).
* BubbleDialogModelHost would not pass on selected-index updates unless
the user changed the index by performing a combobox action (not true

when an Extension removes a bookmark folder).

This also replaces off-by-one index correction changes with CHECKs for
index correctness inside views::Combobox. This turns security bugs into
crash bugs and also is likelier to get us better crash stacks if this
happens in the wild as well.

(cherry picked from commit d2e1d6871cf7ca9dbbc82a400be49234d20f98cf)

~~Bug: 1227777~~
Change-Id: I9b851129fee4bdd249c1db77b01312b6671784be
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018568
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#904551}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3053077
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4577@{#175}
Cr-Branched-From: 761ddde228655e313424edec06497d0c56b0f3c4-refs/heads/master@{#902210}

[modify] https://crrev.com/cb19602196e186a7d2ee5525ddb5d63a416fe9fd/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc
[modify] https://crrev.com/cb19602196e186a7d2ee5525ddb5d63a416fe9fd/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.h
[modify] https://crrev.com/cb19602196e186a7d2ee5525ddb5d63a416fe9fd/ui/views/bubble/bubble_dialog_model_host.cc
[modify] https://crrev.com/cb19602196e186a7d2ee5525ddb5d63a416fe9fd/ui/views/controls/combobox/combobox.cc
[modify] https://crrev.com/cb19602196e186a7d2ee5525ddb5d63a416fe9fd/ui/views/controls/combobox/combobox.h

Comment 27 by amyressler@google.com on Tue, Jul 27, 2021, 4:57 PM EDT Project Member

Labels: -Merge-Request-91 -Merge-Review-92 Merge-Approved-92 Merge-Approved-91

Thanks for merging to M93. Please go ahead and merge to M92, branch 4515 by EOD Thursday, so this can be a part of the stable channel security refresh next week. Additionally, please also merge to M91, branch 4472, as this now the extended stable release branch as we move toward the 4W stable channel release cycle.

Comment 28 by Git Watcher on Tue, Jul 27, 2021, 6:30 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/+/5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730

commit 5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730
Author: Peter Boström <pbos@chromium.org>
Date: Tue Jul 27 22:29:24 2021

Fix RecentlyUsedFoldersComboModel heap overflows

This fixes a few bugs:
* RecentlyUsedFoldersComboModel::RemoveNode() would not inform its
observers of changes.
* RecentlyUsedFoldersComboModel::GetDefaultIndex() did not behave well
after model changes (could end up using a cached out-of-bounds index).
* BubbleDialogModelHost would not pass on selected-index updates unless
the user changed the index by performing a combobox action (not true
when an Extension removes a bookmark folder).

This also replaces off-by-one index correction changes with CHECKs for
index correctness inside views::Combobox. This turns security bugs into
crash bugs and also is likelier to get us better crash stacks if this
happens in the wild as well.

(cherry picked from commit d2e1d6871cf7ca9dbbc82a400be49234d20f98cf)

~~Bug: 1227777~~
Change-Id: I9b851129fee4bdd249c1db77b01312b6671784be
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018568
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#904551}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057514
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4515@{#1848}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc
[modify] https://crrev.com/5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.h
[modify] https://crrev.com/5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730/ui/views/bubble/bubble_dialog_model_host.cc
[modify] https://crrev.com/5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730/ui/views/controls/combobox/combobox.cc
[modify] https://crrev.com/5c37324fc1f3e53a9f4c5fc2f3d17bd2b64c5730/ui/views/controls/combobox/combobox.h

Comment 29 by Git Watcher on Tue, Jul 27, 2021, 7:32 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/dd7b6f26e4768664d743d3c7dd793b82bd814998

commit dd7b6f26e4768664d743d3c7dd793b82bd814998
Author: Peter Boström <pbos@chromium.org>
Date: Tue Jul 27 23:31:44 2021

Fix RecentlyUsedFoldersComboModel heap overflows

This fixes a few bugs:
* RecentlyUsedFoldersComboModel::RemoveNode() would not inform its
observers of changes.
* RecentlyUsedFoldersComboModel::GetDefaultIndex() did not behave well
after model changes (could end up using a cached out-of-bounds index).
* BubbleDialogModelHost would not pass on selected-index updates unless
the user changed the index by performing a combobox action (not true
when an Extension removes a bookmark folder).

This also replaces off-by-one index correction changes with CHECKs for
index correctness inside views::Combobox. This turns security bugs into
crash bugs and also is likelier to get us better crash stacks if this
happens in the wild as well.

(cherry picked from commit d2e1d6871cf7ca9dbbc82a400be49234d20f98cf)

~~Bug: 1237777~~
Change-Id: I9b851129fee4bdd249c1db77b01312b6671784be
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018568
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#904551}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057499
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4472@{#1581}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/dd7b6f26e4768664d743d3c7dd793b82bd814998/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc
[modify] https://crrev.com/dd7b6f26e4768664d743d3c7dd793b82bd814998/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.h
[modify] https://crrev.com/dd7b6f26e4768664d743d3c7dd793b82bd814998/ui/views/bubble/bubble_dialog_model_host.cc
[modify] https://crrev.com/dd7b6f26e4768664d743d3c7dd793b82bd814998/ui/views/controls/combobox/combobox.cc
[modify] https://crrev.com/dd7b6f26e4768664d743d3c7dd793b82bd814998/ui/views/controls/combobox/combobox.h

Comment 30 by amyressler@google.com on Wed, Jul 28, 2021, 4:51 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-20000

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 31 by amyressler@google.com on Wed, Jul 28, 2021, 5:01 PM EDT Project Member

Congratulations, Leecraso and Guang Gong! The VRP Panel has decided to award you $20,000 for this report. Great work and thanks for another stellar report that allowed the team to get to a more comprehensive fix!

Comment 32 by amyressler@google.com on Thu, Jul 29, 2021, 5:50 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 33 by amyressler@chromium.org on Mon, Aug 2, 2021, 10:32 AM EDT Project Member

Labels: Release-1-M92

Comment 34 by amyressler@google.com on Mon, Aug 2, 2021, 10:57 AM EDT Project Member

Labels: CVE-2021-30590 CVE_description-missing

Comment 35 by voit@google.com on Thu, Aug 5, 2021, 12:34 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Small LTS-Complexity-Minimal

Comment 36 by voit@google.com on Thu, Aug 5, 2021, 12:35 AM EDT Project Member

Cc: voit@google.com

Comment 37 by gianluca@google.com on Thu, Aug 5, 2021, 6:21 AM EDT Project Member

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

Comment 38 by Git Watcher on Tue, Aug 10, 2021, 1:44 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/440b019fa3a718d146e30c50eff441de9d42c491

commit 440b019fa3a718d146e30c50eff441de9d42c491
Author: Zakhar Voit <voit@google.com>
Date: Tue Aug 10 05:43:55 2021

[M90-LTS] Fix RecentlyUsedFoldersComboModel heap overflows

This fixes a few bugs:
* RecentlyUsedFoldersComboModel::RemoveNode() would not inform its observers of changes.
* RecentlyUsedFoldersComboModel::GetDefaultIndex() did not behave well after model changes (could end up using a cached out-of-bounds index).
* BubbleDialogModelHost would not pass on selected-index updates unless the user changed the index by performing a combobox action (not true when an Extension removes a bookmark folder).

This also replaces off-by-one index correction changes with CHECKs for index correctness inside views::Combobox. This turns security bugs into crash bugs and also is likelier to get us better crash stacks if this happens in the wild as well.

(cherry picked from commit d2e1d6871cf7ca9dbbc82a400be49234d20f98cf)

~~Bug: 1237777~~
Change-Id: I9b851129fee4bdd249c1db77b01312b6671784be
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018568
Commit-Queue: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#904551}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3073100
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Zakhar Voit <voit@google.com>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1562}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/440b019fa3a718d146e30c50eff441de9d42c491/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.cc
[modify] https://crrev.com/440b019fa3a718d146e30c50eff441de9d42c491/chrome/browser/ui/bookmarks/recently_used_folders_combo_model.h
[modify] https://crrev.com/440b019fa3a718d146e30c50eff441de9d42c491/ui/views/bubble/bubble_dialog_model_host.cc
[modify] https://crrev.com/440b019fa3a718d146e30c50eff441de9d42c491/ui/views/controls/combobox/combobox.cc
[modify] https://crrev.com/440b019fa3a718d146e30c50eff441de9d42c491/ui/views/controls/combobox/combobox.h

Comment 39 by voit@google.com on Thu, Aug 12, 2021, 3:08 AM EDT Project Member

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

Comment 40 by amyressler@google.com on Thu, Aug 26, 2021, 1:09 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 41 by sheriffbot on Fri, Oct 29, 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