Starred by 3 users

Owner:	mastiz@chromium.org
CC:	sky@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Bookmarks
Modified:	Sep 22, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Lacros
Pri:	1
Type:	Bug-Security

Security_Impact-Stable
Security_Severity-Medium
Hotlist-Merge-Approved
reward-7500
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-90
Target-90
merge-merged-4240
LTR-Merged-86
LTS-Security-86
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
Release-0-M91
CVE-2021-30529

Issue 1195278: UAF in bookmark

Reported by super...@gmail.com on Thu, Apr 1, 2021, 11:22 PM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36

Steps to reproduce the problem:
1.load the extension
2.do the step as my follows .mp4 will trigger the uaf

What is the expected behavior?

What went wrong?
BookmarkEditorView::ExecuteCommand will run a message loop,
and node[1] will be destroyed in the message loop.Then uaf will be trigger when access the node.

```
void BookmarkEditorView::ExecuteCommand(int command_id, int event_flags) {
  DCHECK(tree_view_->GetActiveNode());
    LOG(ERROR)<<"in BookmarkEditorView::ExecuteCommand";

  if (command_id == IDS_EDIT) {
    tree_view_->StartEditing(tree_view_->GetActiveNode());
  } else if (command_id == IDS_DELETE) {
      LOG(ERROR)<<"in BookmarkEditorView::ExecuteCommand delete";
    EditorNode* node = tree_model_->AsNode(tree_view_->GetActiveNode()); [1]
    if (!node)
      return;
      LOG(ERROR)<<"bypass 1";
    if (node->value != 0) {
        LOG(ERROR)<<"bypass 2";
      const BookmarkNode* b_node =
          bookmarks::GetBookmarkNodeByID(bb_model_, node->value);
      if (!b_node->children().empty() &&
          !chrome::ConfirmDeleteBookmarkNode(b_node,
                                             GetWidget()->GetNativeWindow())) {
        // The folder is not empty and the user didn't confirm.
        return;
      }
      deletes_.push_back(node->value);
    }
    tree_model_->Remove(node->parent(), node);
  } else {
    DCHECK_EQ(IDS_BOOKMARK_EDITOR_NEW_FOLDER_MENU_ITEM, command_id);
    NewFolder(tree_model_->AsNode(tree_view_->GetActiveNode()));
  }
}
```

I will upload the poc soon

Did this work before? N/A

Chrome version: 89.0.4389.114 Channel: stable
OS Version: OS X 11.2.3
Flash Version:

Comment 1 by sheriffbot on Thu, Apr 1, 2021, 11:23 PM EDT

Labels: external_security_report

Comment 2 by super...@gmail.com on Thu, Apr 1, 2021, 11:39 PM EDT

asan.log
18.2 KB View Download

[Deleted] **extension.js**

[Deleted] **manifest.json**

Comment 3 by super...@gmail.com on Fri, Apr 2, 2021, 12:49 AM EDT

extension.js
644 bytes View Download

manifest.json
356 bytes View Download

[Deleted] **meeting_01.mp4**

Comment 4 by super...@gmail.com on Fri, Apr 2, 2021, 3:18 AM EDT

Screencast 2021-04-02 15_03_46.mp4
3.0 MB View Download

Comment 5 Deleted

Comment 6 by drubery@chromium.org on Mon, Apr 5, 2021, 12:55 PM EDT

Owner: mastiz@chromium.org
Cc: sky@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable
Components: UI>Browser>Bookmarks

Thanks for the report, this reproduced for me. Triaging as medium severity due to the need for a specific malicious extension. Forwarding to bookmarks owners.

mastiz@, sky@ - can you take a look?

Comment 7 by drubery@chromium.org on Mon, Apr 5, 2021, 12:55 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 8 by sheriffbot on Mon, Apr 5, 2021, 1:01 PM EDT

Labels: M-90 Target-90

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

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

Comment 9 by sheriffbot on Mon, Apr 5, 2021, 1:37 PM EDT

Labels: -Pri-2 Pri-1

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

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

Comment 10 by sky@chromium.org on Tue, Apr 6, 2021, 7:46 PM EDT

The right thing is likely to convert ConfirmDeleteBookmarkNode to be async.

Comment 11 by super...@gmail.com on Fri, Apr 9, 2021, 9:08 AM EDT

Hello, could you change the impact OS more widely? I think it's not just impact mac. Thank you!

Comment 12 by mastiz@chromium.org on Fri, Apr 9, 2021, 10:09 AM EDT

Status: Started (was: Assigned)

Comment 13 by mastiz@chromium.org on Fri, Apr 9, 2021, 11:32 AM EDT

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

Comment 14 by Git Watcher on Fri, Apr 9, 2021, 2:46 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a453de0ca590f4341a6d8d32bb5f6525705676de

commit a453de0ca590f4341a6d8d32bb5f6525705676de
Author: Mikel Astiz <mastiz@chromium.org>
Date: Fri Apr 09 18:45:35 2021

[bookmarks] Fix UAF if bookmark deleted during modal confirmation dialog

BookmarkEditorView shows a modal dialog when the user requests to delete
a bookmark folder that is non-empty, for the user to confirm. This
involves a nested message loop, which means that additional changes can
take place, including extensions modifying the bookmark tree.

If the bookmark folder being modified by the user happens to be deleted
(e.g. by an extension) while the confirmation dialog is open, prior to
this patch, the code could dereference freed memory.

In this patch, a safeguard is introduced to fix the issue, which is
achieved by detecting problematic changes based on bookmark IDs (which
are integers and never reused during the lifetime of the browser).

Change-Id: Ife1d005f1b3d8d17b5b5d7c07b538732cd377e13
~~Bug: 1195378~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2818022
Commit-Queue: Mikel Astiz <mastiz@chromium.org>
Reviewed-by: Peter Kasting <pkasting@chromium.org>
Cr-Commit-Position: refs/heads/master@{#871053}

[modify] https://crrev.com/a453de0ca590f4341a6d8d32bb5f6525705676de/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc
[modify] https://crrev.com/a453de0ca590f4341a6d8d32bb5f6525705676de/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/a453de0ca590f4341a6d8d32bb5f6525705676de/chrome/browser/ui/views/bookmarks/bookmark_editor_view.cc
[modify] https://crrev.com/a453de0ca590f4341a6d8d32bb5f6525705676de/chrome/browser/ui/views/bookmarks/bookmark_editor_view.h
[modify] https://crrev.com/a453de0ca590f4341a6d8d32bb5f6525705676de/chrome/browser/ui/views/bookmarks/bookmark_editor_view_unittest.cc

Comment 15 by mastiz@chromium.org on Mon, Apr 12, 2021, 5:19 AM EDT

Status: Fixed (was: Started)
Labels: Merge-Request-91

Comment 16 by sheriffbot on Mon, Apr 12, 2021, 12:36 PM EDT

Labels: reward-topanel

Comment 17 by sheriffbot on Mon, Apr 12, 2021, 1:50 PM EDT

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

Comment 18 by super...@gmail.com on Mon, Apr 12, 2021, 10:50 PM EDT

report credit: koocola(@alo_cook) and Nan Wang(@eternalsakura13) of 360 Alpha Lab.
Thank you!

Comment 19 by sheriffbot on Tue, Apr 13, 2021, 5:22 AM EDT

Labels: -Merge-Request-91 Hotlist-Merge-Approved Merge-Approved-91

Your change meets the bar and is auto-approved for M91. Please go ahead and merge the CL to branch 4472 (refs/branch-heads/4472) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: benmason@(Android), bindusuvarna@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 20 by Git Watcher on Tue, Apr 13, 2021, 4:53 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e4ac01f0725366234305fdd841e87a371c3d3ae3

commit e4ac01f0725366234305fdd841e87a371c3d3ae3
Author: Mikel Astiz <mastiz@chromium.org>
Date: Tue Apr 13 20:52:01 2021

[bookmarks] Fix UAF if bookmark deleted during modal confirmation dialog

BookmarkEditorView shows a modal dialog when the user requests to delete
a bookmark folder that is non-empty, for the user to confirm. This
involves a nested message loop, which means that additional changes can
take place, including extensions modifying the bookmark tree.

If the bookmark folder being modified by the user happens to be deleted
(e.g. by an extension) while the confirmation dialog is open, prior to
this patch, the code could dereference freed memory.

In this patch, a safeguard is introduced to fix the issue, which is
achieved by detecting problematic changes based on bookmark IDs (which
are integers and never reused during the lifetime of the browser).

(cherry picked from commit a453de0ca590f4341a6d8d32bb5f6525705676de)

Change-Id: Ife1d005f1b3d8d17b5b5d7c07b538732cd377e13
~~Bug: 1195378~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2818022
Commit-Queue: Mikel Astiz <mastiz@chromium.org>
Reviewed-by: Peter Kasting <pkasting@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#871053}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2822158
Reviewed-by: Mikel Astiz <mastiz@chromium.org>
Reviewed-by: Prudhvi Kumar Bommana <pbommana@google.com>
Auto-Submit: Mikel Astiz <mastiz@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Owners-Override: Prudhvi Kumar Bommana <pbommana@google.com>
Cr-Commit-Position: refs/branch-heads/4472@{#43}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/e4ac01f0725366234305fdd841e87a371c3d3ae3/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc
[modify] https://crrev.com/e4ac01f0725366234305fdd841e87a371c3d3ae3/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/e4ac01f0725366234305fdd841e87a371c3d3ae3/chrome/browser/ui/views/bookmarks/bookmark_editor_view.cc

[modify] https://crrev.com/e4ac01f0725366234305fdd841e87a371c3d3ae3/chrome/browser/ui/views/bookmarks/bookmark_editor_view.h
[modify] https://crrev.com/e4ac01f0725366234305fdd841e87a371c3d3ae3/chrome/browser/ui/views/bookmarks/bookmark_editor_view_unittest.cc

Comment 21 by amyressler@google.com on Thu, Apr 22, 2021, 7:56 PM EDT

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 22 by amyressler@chromium.org on Fri, Apr 23, 2021, 6:14 PM EDT

Congratulations, superjoe@! The VRP Panel has decided to award you $7500 for this report. Nice work and thanks for reporting this!

Comment 23 by super...@gmail.com on Fri, Apr 23, 2021, 10:30 PM EDT

Thank you very much!

Comment 24 by amyressler@google.com on Mon, Apr 26, 2021, 10:34 AM EDT

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@chromium.org on Mon, May 24, 2021, 11:11 AM EDT

Labels: Release-0-M91

Comment 26 by amyressler@google.com on Mon, May 24, 2021, 2:18 PM EDT

Labels: CVE-2021-30529 CVE_description-missing

Comment 27 by janag...@google.com on Wed, May 26, 2021, 10:23 AM EDT

Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 28 by gianluca@google.com on Wed, May 26, 2021, 11:47 AM EDT

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 29 by Git Watcher on Thu, May 27, 2021, 11:28 AM EDT

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/10bd177a4b078b47636c3894daf0f3b5af348733

commit 10bd177a4b078b47636c3894daf0f3b5af348733
Author: Mikel Astiz <mastiz@chromium.org>
Date: Thu May 27 15:27:22 2021

[86-LTS][bookmarks] Fix UAF if bookmark deleted during modal confirmation dialog

BookmarkEditorView shows a modal dialog when the user requests to delete
a bookmark folder that is non-empty, for the user to confirm. This
involves a nested message loop, which means that additional changes can
take place, including extensions modifying the bookmark tree.

If the bookmark folder being modified by the user happens to be deleted
(e.g. by an extension) while the confirmation dialog is open, prior to
this patch, the code could dereference freed memory.

In this patch, a safeguard is introduced to fix the issue, which is
achieved by detecting problematic changes based on bookmark IDs (which
are integers and never reused during the lifetime of the browser).

(cherry picked from commit a453de0ca590f4341a6d8d32bb5f6525705676de)

Change-Id: Ife1d005f1b3d8d17b5b5d7c07b538732cd377e13
~~Bug: 1195278~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2818022
Commit-Queue: Mikel Astiz <mastiz@chromium.org>
Reviewed-by: Peter Kasting <pkasting@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#871053}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2919850
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Jana Grill <janagrill@google.com>
Owners-Override: Jana Grill <janagrill@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1651}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/10bd177a4b078b47636c3894daf0f3b5af348733/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc
[modify] https://crrev.com/10bd177a4b078b47636c3894daf0f3b5af348733/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/10bd177a4b078b47636c3894daf0f3b5af348733/chrome/browser/ui/views/bookmarks/bookmark_editor_view.cc
[modify] https://crrev.com/10bd177a4b078b47636c3894daf0f3b5af348733/chrome/browser/ui/views/bookmarks/bookmark_editor_view.h
[modify] https://crrev.com/10bd177a4b078b47636c3894daf0f3b5af348733/chrome/browser/ui/views/bookmarks/bookmark_editor_view_unittest.cc

Comment 30 by janag...@google.com on Thu, May 27, 2021, 11:37 AM EDT

Labels: -LTS-Merge-Approved-86 LTR-Merged-86

Comment 31 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by vsavu@google.com on Mon, Jun 14, 2021, 12:29 PM EDT

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 33 by gianluca@google.com on Tue, Jun 15, 2021, 6:28 AM EDT

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

Comment 34 by Git Watcher on Wed, Jun 16, 2021, 9:03 AM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0b4f280e4578b5e185ffc2a3e6d4aebb98869d87

commit 0b4f280e4578b5e185ffc2a3e6d4aebb98869d87
Author: Mikel Astiz <mastiz@chromium.org>
Date: Wed Jun 16 13:02:07 2021

[M90-LTS][bookmarks] Fix UAF if bookmark deleted during modal confirmation dialog

BookmarkEditorView shows a modal dialog when the user requests to delete
a bookmark folder that is non-empty, for the user to confirm. This
involves a nested message loop, which means that additional changes can
take place, including extensions modifying the bookmark tree.

If the bookmark folder being modified by the user happens to be deleted
(e.g. by an extension) while the confirmation dialog is open, prior to
this patch, the code could dereference freed memory.

In this patch, a safeguard is introduced to fix the issue, which is
achieved by detecting problematic changes based on bookmark IDs (which
are integers and never reused during the lifetime of the browser).

(cherry picked from commit a453de0ca590f4341a6d8d32bb5f6525705676de)

Change-Id: Ife1d005f1b3d8d17b5b5d7c07b538732cd377e13
~~Bug: 1195276~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2818022
Commit-Queue: Mikel Astiz <mastiz@chromium.org>
Reviewed-by: Peter Kasting <pkasting@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#871053}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2961090
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1526}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/0b4f280e4578b5e185ffc2a3e6d4aebb98869d87/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc
[modify] https://crrev.com/0b4f280e4578b5e185ffc2a3e6d4aebb98869d87/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/0b4f280e4578b5e185ffc2a3e6d4aebb98869d87/chrome/browser/ui/views/bookmarks/bookmark_editor_view.cc
[modify] https://crrev.com/0b4f280e4578b5e185ffc2a3e6d4aebb98869d87/chrome/browser/ui/views/bookmarks/bookmark_editor_view.h
[modify] https://crrev.com/0b4f280e4578b5e185ffc2a3e6d4aebb98869d87/chrome/browser/ui/views/bookmarks/bookmark_editor_view_unittest.cc

Comment 35 by vsavu@google.com on Wed, Jun 16, 2021, 9:04 AM EDT
Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 36 by sheriffbot on Wed, Sep 22, 2021, 1:34 PM EDT
Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

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