☆ Starred by 4 users

Owner:	nasko@chromium.org **Out until Jan 2023**
CC:	calamity@chromium.org adetaylor@chromium.org carlosil@chromium.org johntlee@chromium.org sky@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Bookmarks
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Arch-x86_64
Deadline-Exceeded
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
Target-94
Target-93
M-96
Target-96
FoundIn-93
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
merge-merged-4692
merge-merged-97

merge-merged-4758
merge-merged-98
Release-0-M97

Issue 1249426: heap buffer overflow in BookmarkManagerPrivateDropFunction::RunOnReady

Reported by wxhu...@gmail.com on Tue, Sep 14, 2021, 7:55 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36

Steps to reproduce the problem:

```
  size_t drop_index;
  if (params->index)
    drop_index = static_cast<size_t>(*params->index);
  else
    drop_index = drop_parent->children().size();

  BookmarkManagerPrivateDragEventRouter* router =
      BookmarkManagerPrivateDragEventRouter::FromWebContents(web_contents);

  DCHECK(router);
  const BookmarkNodeData* drag_data = router->GetBookmarkNodeData();
  DCHECK_NE(nullptr, drag_data) << "Somehow we're dropping null bookmark data";
  const bool copy = false;
  chrome::DropBookmarks(
      GetProfile(), *drag_data, drop_parent, drop_index, copy);
```

here we could control the drop_index

and in this function ```chrome::DropBookmarks``` it will enter the code

```
        if (copy) {
          model->Copy(dragged_nodes[i], parent_node, index);
        } else {
          model->Move(dragged_nodes[i], parent_node, index);
```

so I here if we set a large index to the function copy, we may cause heap overflow, but for convincidence
I change the unit_test and change the code

```
 model_->Copy(node_to_copy, destination, 1);
```

to

```
 model_->Copy(node_to_copy, destination, 100);
```

https://source.chromium.org/chromium/chromium/src/+/main:components/bookmarks/browser/bookmark_model_unittest.cc;l=1056;drc=08383dad191fd0106d20f9ac06981b8cc89ed09b;bpv=0;bpt=1

here is the asan output.

What is the expected behavior?

What went wrong?
above all

Did this work before? N/A

Chrome version: 93.0.4577.82 Channel: stable
OS Version: 10.0

asan.txt
16.4 KB View Download

Comment 1 by sheriffbot on Tue, Sep 14, 2021, 8:00 AM EDT   Project Member

Labels: external_security_report

Comment 2 by carlosil@chromium.org on Tue, Sep 14, 2021, 5:49 PM EDT   Project Member

Labels: Needs-Feedback

Thanks for the report, do you have a PoC that triggers the bug?

Comment 3 by wxhu...@gmail.com on Tue, Sep 14, 2021, 6:37 PM EDT

Haven't try it. But from the code, it has the vul.

Comment 4 by sheriffbot on Tue, Sep 14, 2021, 6:43 PM EDT   Project Member

Cc: carlosil@chromium.org
Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 5 by wxhu...@gmail.com on Wed, Sep 15, 2021, 10:32 AM EDT

I begin to try it, and I find the api ```chrome.bookmarkManagerPrivate.drop``` can use in "chrome://bookmarks/".
and my analyse before seems a little wrong. because it will enter the code

```
model->Move(dragged_nodes[i], parent_node, index);
```

rather then copy(), but anyway, it still will cause heap overflow. I will keep to try it. wait serveral hours.

Comment 6 by wxhu...@gmail.com on Wed, Sep 15, 2021, 11:58 AM EDT

step to reproduce
- enter chrome://bookmarks
- open devtools, execute js ```chrome.bookmarkManagerPrivate.getSubtree("0", false, function(result){console.log(result);});```
- we can get the bookmark id, the we execute js

```
chrome.bookmarkManagerPrivate.onDrop.addListener(function(){chrome.bookmarkManagerPrivate.drop("5", 1000);});
```

- then we drage the bookmark and drop it.
- then browser crash.

asan.txt
12.9 KB View Download

Comment 7 by wxhu...@gmail.com on Wed, Sep 15, 2021, 12:00 PM EDT

oh, you should notice the js ,

```
chrome.bookmarkManagerPrivate.onDrop.addListener(function(){chrome.bookmarkManagerPrivate.drop("5", 1000);});
```

the number of "5" that I get it from this js.

~~~
```chrome.bookmarkManagerPrivate.getSubtree("0", false, function(result){console.log(result);});```
~~~

Comment 8 by carlosil@chromium.org on Wed, Sep 15, 2021, 7:15 PM EDT Project Member

Labels: Needs-Feedback

I can't reproduce with the steps in comment 6, it just triggers the DCHECK (DCHECK_NE(nullptr, drag_data) << "Somehow we're dropping null bookmark data";)

As far as the reproduction from the unit test, how would this be replicated in the open? It doesn't seem like drop_index can be controlled by the renderer.

Comment 9 by wxhu...@gmail.com on Wed, Sep 15, 2021, 7:25 PM EDT

you should get the bookmarks parents id bythe step of comment 7

Comment 10 by sheriffbot on Wed, Sep 15, 2021, 7:28 PM EDT Project Member

Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 11 by carlosil@chromium.org on Wed, Sep 15, 2021, 7:33 PM EDT Project Member

Labels: Needs-Feedback

I'm doing the id step, but it still only results in the DCHECK

Comment 12 by wxhu...@gmail.com on Wed, Sep 15, 2021, 7:38 PM EDT

maybe you should use the release asan build?

Comment 13 by sheriffbot on Wed, Sep 15, 2021, 7:42 PM EDT Project Member

Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 14 by carlosil@chromium.org on Thu, Sep 16, 2021, 4:26 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: sky@chromium.org

Labels: FoundIn-93 Security_Severity-High

Components: UI>Browser>Bookmarks

Yeah, was able to reproduce on Release.

sky: Could you PTAL since this is similar to ~~crbug.com/1223667~~. Thanks

Comment 15 by sheriffbot on Thu, Sep 16, 2021, 4:28 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 16 by sky@chromium.org on Thu, Sep 16, 2021, 11:25 PM EDT Project Member

Cc: calamity@chromium.org

This can definitely trigger bad behavior, but I'm wondering if these matter. Aren't these functions only exposed to internal pages? Isn't this only exposed to the bookmark manager? Chris, do I have this right?

Comment 17 by calamity@chromium.org on Fri, Sep 17, 2021, 6:43 AM EDT Project Member

Yes, the BookmarkManagerPrivateAPI should only be exposed to chrome://bookmarks and chrome://read-later.top-chrome.

https://source.chromium.org/chromium/chromium/src/+/main:chrome/common/extensions/api/_api_features.json;l=123?q=_api_features.json&ss=chromium%2Fchromium%2Fsrc

Comment 18 by sky@chromium.org on Fri, Sep 17, 2021, 11:41 AM EDT Project Member

So, I think that means we don't really care about this, and can close as won't fix. Do I have that right?

Comment 19 by sky@chromium.org on Fri, Sep 17, 2021, 11:42 AM EDT Project Member

Said differently, this code should be able to assume it was passed valid parameters, right?

Comment 20 by wxhu...@gmail.com on Fri, Sep 17, 2021, 12:28 PM EDT

interesting question ☺

Comment 21 by sheriffbot on Fri, Sep 17, 2021, 12:47 PM EDT Project Member

Labels: M-93 Target-93

Setting milestone and target because of high severity.

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

Comment 22 by sheriffbot on Fri, Sep 17, 2021, 1:07 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 23 by calamity@chromium.org on Sun, Sep 19, 2021, 8:51 PM EDT Project Member

Cc: johntlee@chromium.org

#19: As I understand it, from a security model perspective, we treat chrome:// WebUIs as part of the browser. i.e the code is trusted to Do The Right Thing, and we do not program APIs defensively.

I would be comfortable closing this as WontFix. cc-ing current OWNER of chrome://bookmarks in case they're interested.

Comment 24 by sheriffbot on Wed, Sep 22, 2021, 12:21 PM EDT Project Member

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

Comment 25 by sky@chromium.org on Wed, Sep 22, 2021, 1:34 PM EDT Project Member

Status: WontFix (was: Assigned)

I'm closing. Please reopen if this is wrong.

Comment 26 by sky@chromium.org on Wed, Sep 22, 2021, 1:34 PM EDT Project Member

Cc: sky@chromium.org

~~Issue 1249874~~ has been merged into this issue.

Comment 27 by wxhu...@gmail.com on Wed, Sep 22, 2021, 6:38 PM EDT

Can I disclose the detail of the bug as you set the bug to won't fix

Comment 28 by sky@chromium.org on Wed, Sep 22, 2021, 6:48 PM EDT Project Member

Cc: adetaylor@chromium.org

Someone from the security team should answer that.

Comment 29 by wxhu...@gmail.com on Fri, Sep 24, 2021, 2:17 AM EDT

I will send a email to adetaylor@ to ask him about comment#27.

Comment 30 by nasko@chromium.org on Fri, Sep 24, 2021, 1:52 PM EDT Project Member

Status: Untriaged (was: WontFix)

I agree that WebUIs are chrome internal and we don't expect bad inputs. We have seen in the past exploits that involve WebUI in a multistep exploit chain, so I would prefer if we can fix issues in WebUIs, even if they aren't immediately reachable, especially if we have a simple fix.

In this case, can't we just convert the DCHECK_NE that carlosil@ mentioned is triggered into a CHECK? It seems like a trivial change and it will convert the potential exploitable condition into a crash, which is much better for security. Since we don't expect Chrome's internal code to violate that condition, we don't get any real crashes for users in regular operation.

Does this sound reasonable?

Comment 31 by sheriffbot on Fri, Sep 24, 2021, 2:16 PM EDT Project Member

Status: Assigned (was: Untriaged)

Comment 32 by sky@chromium.org on Wed, Sep 29, 2021, 6:27 PM EDT Project Member

Owner: nasko@chromium.org

That sounds perfectly reasonable Nasko. My take from briefly looking at the code is that it was not designed with what you outlined. Rather it's a mix of no checks at all or DCHECKs. I think someone needs to go through all the private apis exposed and ensure they are consistent. I'm going to kick this to Nasko as I think it requires a more concerted effort.

Comment 33 by sheriffbot on Sat, Oct 9, 2021, 12:21 PM EDT Project Member

nasko: 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 34 by sheriffbot on Sat, Oct 23, 2021, 12:21 PM EDT Project Member

nasko: Uh oh! This issue still open and hasn't been updated in the last 28 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 35 by sky@chromium.org on Fri, Oct 29, 2021, 4:15 PM EDT Project Member

~~Issue 1264822~~ has been merged into this issue.

Comment 36 by sheriffbot on Mon, Nov 15, 2021, 12:22 PM EST Project Member

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

Comment 37 by sheriffbot on Mon, Nov 15, 2021, 1:51 PM EST Project Member

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

Comment 38 by Git Watcher on Thu, Dec 9, 2021, 9:11 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7c66fad9cd7633ed04890e84cc0c13b26b5cce1c

commit 7c66fad9cd7633ed04890e84cc0c13b26b5cce1c
Author: Nasko Oskov <nasko@chromium.org>
Date: Fri Dec 10 02:10:34 2021

Convert DCHECK to CHECK in Bookmark Manager

This CL converts a DCHECK into a more stringent CHECK to ensure we crash
the browser process instead of hitting a use-after-free condition.

~~Bug: 1249426~~
Change-Id: I919bfc4dcd11b8acccf217f5000fe7f1fbec7e6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3323662
Reviewed-by: John Lee <johntlee@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Nasko Oskov <nasko@chromium.org>
Cr-Commit-Position: refs/heads/main@{#950388}

[modify]
https://crrev.com/7c66fad9cd7633ed04890e84cc0c13b26b5cce1c/chrome/browser/extensions/api/bookmark_manager_private/bookmark_manager_private_api.cc

Comment 39 by nasko@chromium.org on Mon, Dec 13, 2021, 12:42 PM EST Project Member

Status: Fixed (was: Assigned)

The change in #38 has stuck over the last few days, therefore resolving as fixed.

Comment 40 by sheriffbot on Mon, Dec 13, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 41 by sheriffbot on Mon, Dec 13, 2021, 1:41 PM EST Project Member

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

Comment 42 by sheriffbot on Mon, Dec 13, 2021, 2:02 PM EST Project Member

Labels: Merge-Request-96 Merge-Request-97 Merge-Request-98

Requesting merge to stable M96 because latest trunk commit (950388) appears to be after stable branch point (929512).

Requesting merge to beta M97 because latest trunk commit (950388) appears to be after beta branch point (938553).

Requesting merge to dev M98 because latest trunk commit (950388) appears to be after dev branch point (950365).

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

Comment 43 by sheriffbot on Mon, Dec 13, 2021, 2:08 PM 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 44 by sheriffbot on Mon, Dec 13, 2021, 2:08 PM EST Project Member

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

Merge review required: M97 is already shipping to beta.

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
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 45 by sheriffbot on Mon, Dec 13, 2021, 2:08 PM EST Project Member

Labels: -Merge-Request-96 Merge-Review-96

Merge review required: M96 is already shipping to stable.

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
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: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 46 by adetaylor@google.com on Mon, Dec 13, 2021, 2:40 PM EST Project Member

Labels: -Merge-Review-96 -Merge-Review-97 Merge-Approved-96 Merge-Approved-97

Approving merge to M96 (branch 4664) and M97 (branch 4692). Please go ahead and merge assuming no crashes showed up in Canary over the weekend.

Comment 47 by srinivassista@google.com on Tue, Dec 14, 2021, 1:14 PM EST Project Member

This issue has been approved for Merge to M98, we are cutting the RC build tomorrow for dev release (this will be last release before holidays so please help compelete your merge before EOD dec 14, so we can include in dev release.

Comment 48 by Git Watcher on Tue, Dec 14, 2021, 2:51 PM EST Project Member

Labels: -merge-approved-96 merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/875cf9db390cfab678180aa3719d8a14ec519199

commit 875cf9db390cfab678180aa3719d8a14ec519199
Author: Nasko Oskov <nasko@chromium.org>
Date: Tue Dec 14 19:49:55 2021

[M96] Convert DCHECK to CHECK in Bookmark Manager

This CL converts a DCHECK into a more stringent CHECK to ensure we crash
the browser process instead of hitting a use-after-free condition.

(cherry picked from commit 7c66fad9cd7633ed04890e84cc0c13b26b5cce1c)

~~Bug: 1249426~~
Change-Id: I919bfc4dcd11b8acccf217f5000fe7f1fbec7e6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3323662
Reviewed-by: John Lee <johntlee@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Nasko Oskov <nasko@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#950388}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3336863
Auto-Submit: Nasko Oskov <nasko@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Commit-Position: refs/branch-heads/4664@{#1305}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/875cf9db390cfab678180aa3719d8a14ec519199/chrome/browser/extensions/api/bookmark_manager_private/bookmark_manager_private_api.cc

Comment 49 by Git Watcher on Tue, Dec 14, 2021, 3:19 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/+/a61ca664b411b5d78a39f7038b4037e80ce4faa1

commit a61ca664b411b5d78a39f7038b4037e80ce4faa1
Author: Nasko Oskov <nasko@chromium.org>
Date: Tue Dec 14 20:18:26 2021

[M97] Convert DCHECK to CHECK in Bookmark Manager

This CL converts a DCHECK into a more stringent CHECK to ensure we crash
the browser process instead of hitting a use-after-free condition.

(cherry picked from commit 7c66fad9cd7633ed04890e84cc0c13b26b5cce1c)

~~Bug: 1249426~~
Change-Id: I919bfc4dcd11b8acccf217f5000fe7f1fbec7e6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3323662
Reviewed-by: John Lee <johntlee@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Nasko Oskov <nasko@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#950388}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3336897
Auto-Submit: Nasko Oskov <nasko@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Commit-Position: refs/branch-heads/4692@{#981}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify]
https://crrev.com/a61ca664b411b5d78a39f7038b4037e80ce4faa1/chrome/browser/extensions/api/bookmark_manager_private/bookmark_manager_private_api.cc

Comment 50 by Git Watcher on Tue, Dec 14, 2021, 3:27 PM 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/+/8f92f216b788253fb0d2b06929129209d01ed233

commit 8f92f216b788253fb0d2b06929129209d01ed233
Author: Nasko Oskov <nasko@chromium.org>
Date: Tue Dec 14 20:26:46 2021

[M98] Convert DCHECK to CHECK in Bookmark Manager

This CL converts a DCHECK into a more stringent CHECK to ensure we crash
the browser process instead of hitting a use-after-free condition.

(cherry picked from commit 7c66fad9cd7633ed04890e84cc0c13b26b5cce1c)

~~Bug: 1249426~~
Change-Id: I919bfc4dcd11b8acccf217f5000fe7f1fbec7e6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3323662
Reviewed-by: John Lee <johntlee@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Nasko Oskov <nasko@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#950388}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3339653
Auto-Submit: Nasko Oskov <nasko@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Commit-Position: refs/branch-heads/4758@{#41}
Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify]

https://crrev.com/8f92f216b788253fb0d2b06929129209d01ed233/chrome/browser/extensions/api/bookmark_manager_private/bookmark_manager_private_api.cc

Comment 51 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:29 PM EST Project Member

Labels: Release-0-M97

Comment 52 by amyressler@google.com on Tue, Jan 4, 2022, 1:33 PM EST Project Member

Labels: CVE-2022-0101 CVE_description-missing

Comment 53 by amyressler@google.com on Wed, Jan 5, 2022, 8:01 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 54 by amyressler@chromium.org on Wed, Jan 5, 2022, 8:17 PM EST Project Member

Congratulations, the VRP Panel has decided to award you $1,000 for this report to thank you for your efforts!

Comment 55 by wxhu...@gmail.com on Thu, Jan 6, 2022, 1:54 AM EST

Thank you!

Comment 56 by amyressler@google.com on Thu, Jan 6, 2022, 4:16 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 57 by sheriffbot on Tue, Mar 22, 2022, 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

Comment 58 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted