Starred by 3 users

Owner:	lazyboy@chromium.org
CC:	rzanoni@google.com rdevl...@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions>API
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
reward-5000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
FoundIn-75
external_security_report
Target-100
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1488

Issue 1302959: Security: Extension permission escalation

Reported by t...@wavebox.io on Fri, Mar 4, 2022, 7:19 AM EST

Code

VULNERABILITY DETAILS
Please provide a brief explanation of the security issue.

An extension with no tabs permission is able to access url, pendingUrl, title & faviconUrl through the change events

VERSION
Chrome Version: [99.0.4844.51] + [stable]
Operating System: [all]

REPRODUCTION CASE

Attached are two extensions (prefixed ext1 and ext2). Ext2 has tabs permission, ext1 does not.

tabs.onUpdated leaks information destined for other tabs in the form of supplying additional arguments to the callback (such as tabs with extra details). Depending on the load order of the extensions, dictates whether the extension will receive the additional information.

Attached are two extensions (prefixed with ext1 and ext2). When ext1 loads, it binds onto tabs.onUpdated. If it only receives two arguments, it reloads the extension to ensure it's loaded last and hence can exploit this bug.

To demonstrate the bug, load both ext1 and ext2 extensions into Chrome. (You will need to place ext1 in a folder and rename ext1_manifest.json to be manifest. Then do the same with ext2). Then create, reload or navigate a tab. Ext1 logs the leaked information in the background dev tools.

CREDIT INFORMATION
Reporter credit: tom@wavebox.io

ext1_background.js
289 bytes View Download

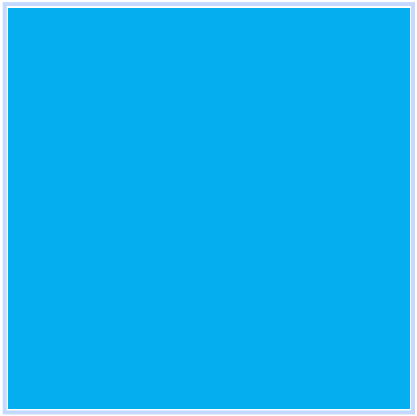
ext1_manifest.json
335 bytes View Download

ext2_background.js
46 bytes View Download

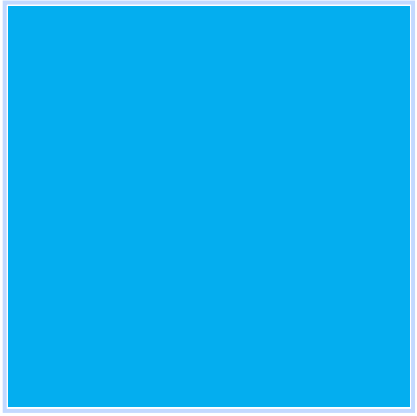
ext2_manifest.json
343 bytes View Download

icon_16.png
531 bytes View Download

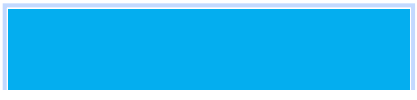
icon_32.png
551 bytes View Download



icon_48.png
639 bytes View Download



icon_128.png
923 bytes View Download



Comment 1 by sheriffbot on Fri, Mar 4, 2022, 7:22 AM EST Project Member

Labels: external_security_report

Comment 2 by t...@wavebox.io on Fri, Mar 4, 2022, 9:02 AM EST

Just looking at ways this could be patched. You could change WillDispatchTabUpdatedEvent in chrome/browser/extensions/api/tabs/tabs_event_router.cc to clear the list and re-populate when executing...

```
bool WillDispatchTabUpdatedEvent(
    WebContents* contents,
    const std::set<std::string> changed_property_names,
    content::BrowserContext* browser_context,
    Feature::Context target_context,
    const Extension* extension,
    Event* event,
    const base::DictionaryValue* listener_filter) {
  ExtensionTabUtil::ScrubTabBehavior scrub_tab_behavior =
      ExtensionTabUtil::GetScrubTabBehavior(extension, target_context,
                                            contents);
  std::unique_ptr<api::tabs::Tab> tab_object =
      ExtensionTabUtil::CreateTabObject(contents, scrub_tab_behavior,
                                        extension);

  std::unique_ptr<base::DictionaryValue> tab_value = tab_object->ToValue();

  auto changed_properties = std::make_unique<base::DictionaryValue>();
  const base::Value* value = nullptr;
  for (const auto& property : changed_property_names) {
    if (tab_value->Get(property, &value))
      changed_properties->SetKey(property, value->Clone());
  }

+  event->event_args->ClearList();
+  event->event_args->Append(ExtensionTabUtil::GetTabId(contents));
  event->event_args->Append(std::move(changed_properties));
  event->event_args->Append(std::move(tab_value));
  return true;
}
```

Comment 3 by dcheng@chromium.org on Fri, Mar 4, 2022, 5:45 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: rdevl...@chromium.org
Labels: Security_Severity-Medium FoundIn-75 OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: Platform>Extensions>API

I'm able to reproduce. I had to edit the extension manifest a bit to remove the icons, but I can confirm that the URL is present in the tab events for the extension with no tabs permission.
https://developer.chrome.com/docs/extensions/reference/tabs/ says "However, if you require access to the url, pendingUrl, title, or favIconUrl properties of tabs.Tab, you must declare the "tabs" permission in the manifest" so this seems like an infoleak.

Comment 4 by dcheng@chromium.org on Fri, Mar 4, 2022, 5:45 PM EST Project Member

Note: I also commented out the branches for chrome.runtime.reload() and just (re)loaded the extensions in various orders to try triggering the bug.

Comment 5 by sheriffbot on Fri, Mar 4, 2022, 5:46 PM EST Project Member

Labels: Security_Impact-Extended

Comment 6 by sheriffbot on Sat, Mar 5, 2022, 12:51 PM EST Project Member

Labels: M-100 Target-100

Setting milestone and target because of medium severity.

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

Comment 7 by rdevl...@chromium.org on Thu, Mar 10, 2022, 5:14 PM EST Project Member

Owner: lazyboy@chromium.org
Cc: rdevl...@chromium.org

Oof, that's awful. It's also been there for a very, very long time - I'm surprised this was never caught before.

I think we should change the will_dispatch_callback to make it clear when the event is changed and when it's not. I think the only modifications to the event that these callbacks do is to mutate the arguments sent to the event and the filter associated with the event. Instead of having them modify the event directly (which affects future listeners, as in this bug), I'd propose we change the signature of WillDispatchCallback to instead take in an "event_args_out" and "event_filter_out" that they can modify, and we use these iff they're set by the callback. This would fix the issue for the tabs API as well as any other API that's mistakenly triggering this behavior.

lazyboy@, do you have the bandwidth to look into this one?

Comment 8 by lazyboy@chromium.org on Thu, Mar 10, 2022, 8:38 PM EST Project Member

Status: Started (was: Assigned)

Comment 9 by Git Watcher on Fri, Mar 25, 2022, 7:45 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/940ddcfaff7bca60f7df77e54735c4f808933bfa

commit 940ddcfaff7bca60f7df77e54735c4f808933bfa
Author: Istiaque Ahmed <lazyboy@chromium.org>
Date: Fri Mar 25 23:44:41 2022

[Extensions] Fix inadvertent leakage of info through event listeners.

Different extension event implementations (e.g. tabs.onCreated) can tweak their listener params through Event::WillDispatchCallback callback. It does so by passing mutable Event* to WillDispatchCallback. This can lead to one extension's event listener inadvertently affecting a different extension's event listener, as the (modified) `Event*` is carried over to next/subsequent listeners.

This CL changes this by removing the mutable Event param from WillDispatchCallback, and exposes "writable" `event_args_out` and `event_filtering_info_out` params to WillDispatchCallback. This is done so that interested parties can set those modified params to be used by dispatcher (EventRouter::DispatchExtensionMessage).

Note that events funneled through LazyEventDispatcher is not currently susceptible to this problem as it copies Event-s before dispatching them.

~~Bug: 1302959~~
Change-Id: I1fbb9b9b29ff2f05c620f2a64f875d83db472136
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3531082
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Commit-Queue: Istiaque Ahmed <lazyboy@chromium.org>
Cr-Commit-Position: refs/heads/main@{#985564}

[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/chrome/browser/extensions/api/tabs/windows_event_router.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/api/audio/audio_api.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/event_router.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/api/printer_provider/printer_provider_api.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/api/usb/usb_device_manager.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/events/lazy_event_dispatcher.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/chrome/browser/extensions/api/downloads/downloads_api.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/event_router.h
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/chrome/browser/extensions/api/tabs/tabs_event_router.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/extensions/browser/api/hid/hid_device_manager.cc
[modify] https://crrev.com/940ddcfaff7bca60f7df77e54735c4f808933bfa/chrome/browser/extensions/api/tabs/tabs_apitest.cc

Comment 10 by lazyboy@chromium.org on Fri, Apr 1, 2022, 8:42 PM EDT Project Member

Status: Fixed (was: Started)

Comment 11 by sheriffbot on Sat, Apr 2, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

.

Comment 12 by sheriffbot on Sat, Apr 2, 2022, 1:39 PM EDT Project Member

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

Comment 13 by amyressler@chromium.org on Mon, Apr 11, 2022, 6:47 PM EDT Project Member

Labels: Merge-Request-101

This fix has only made it to M102 so far, so adding merge-request for M101 since Sheriffbot is sleeping on the job on some Medium severity issues

Comment 14 by sheriffbot on Mon, Apr 11, 2022, 8:16 PM EDT Project Member

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: M101 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), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 15 by amyressler@chromium.org on Tue, Apr 12, 2022, 1:56 PM EDT Project Member

Labels: -Merge-Review-101 Merge-Approved-101

given this fix has been on Canary for almost three weeks, tentatively approving for merge to M101; please confirm there are no stability issues or other concerns and merge this fix to branch 4951 ASAP so this fix can be included in tomorrow's M101 beta release -- thank you

Comment 16 by lazyboy@chromium.org on Tue, Apr 12, 2022, 3:53 PM EDT Project Member

@c#15, on it.

Answering c#14:
1. Y, security issue
2. https://chromium-review.googlesource.com/c/chromium/src/+/3531082
3. Y
5. N/A
6. c#0 steps should suffice

Comment 17 by Git Watcher on Tue, Apr 12, 2022, 7:15 PM EDT Project Member

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f1359aac0f3511fe435c3133bdd550ecf73e8c9a

commit f1359aac0f3511fe435c3133bdd550ecf73e8c9a
Author: Istiaque Ahmed <lazyboy@chromium.org>
Date: Tue Apr 12 23:14:54 2022

[Merge m101][Extensions] Fix inadvertent leakage of info through event listeners.

Different extension event implementations (e.g. tabs.onCreated) can
tweak their listener params through Event::WillDispatchCallback
callback. It does so by passing mutable Event* to
WillDispatchCallback. This can lead to one extension's
event listener inadvertently affecting a different extension's
event listener, as the (modified) `Event*` is carried over to
next/subsequent listeners.

This CL changes this by removing the mutable Event param from
WillDispatchCallback, and exposes "writable" `event_args_out`
and `event_filtering_info_out` params to WillDispatchCallback. This
is done so that interested parties can set those modified params
to be used by dispatcher (EventRouter::DispatchExtensionMessage).

Note that events funneled through LazyEventDispatcher is not
currently susceptible to this problem as it copies Event-s before
dispatching them.

(cherry picked from commit 940ddcfaff7bca60f7df77e54735c4f808933bfa)

~~Bug: 1302959~~
Change-Id: I07c2bfd68b62412f93dcb5fd46315e3b4b496ddd
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3531082
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Commit-Queue: Istiaque Ahmed <lazyboy@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#985564}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3584544
Reviewed-by: David Bertoni <dbertoni@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#707}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify] https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/api/audio/audio_api.cc
[modify]
https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/chrome/browser/extensions/api/tabs/windows_event_router.cc
[modify] https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/event_router.cc
[modify]
https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/events/lazy_event_dispatcher.cc
[modify]
https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/api/printer_provider/printer_provider_api.cc
[modify]
https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/api/usb/usb_device_manager.cc
[modify]

https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/chrome/browser/extensions/api/downloads/downloads_api.cc
[modify] https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/event_router.h
[modify] https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/chrome/browser/extensions/api/tabs/tabs_event_router.cc
[modify] https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/extensions/browser/api/hid/hid_device_manager.cc
[modify] https://crrev.com/f1359aac0f3511fe435c3133bdd550ecf73e8c9a/chrome/browser/extensions/api/tabs/tabs_apitest.cc

Comment 18 by sheriffbot on Tue, Apr 12, 2022, 7:19 PM EDT Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 19 by rzanoni@google.com on Wed, Apr 13, 2022, 8:53 AM EDT Project Member

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 20 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 21 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:12 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $5,000 for this report. A member of our finance team will be in touch to arrange payment. In the interim, please let us know the name/tag/handle/other identifier you would like us to use in acknowledging you for this discovery. Thank you for your efforts and reporting this issue to us!

Comment 22 by t...@wavebox.io on Fri, Apr 15, 2022, 4:34 PM EDT

Thank you, and really great to be able to report this and see it fixed :-).

Can I use "Thomas Beverley from Wavebox.io" as the acknowledgement?

Can I use "Thomas Beverley from Wavebox.io" as the acknowledgement?

Comment 23 by amyressler@chromium.org on Fri, Apr 15, 2022, 5:00 PM EDT Project Member

Sure thing - when the patch for this issue ships in a Stable channel release (should be M101 Stable release on 26 April) you'll be acknowledged accordingly as requested. :)

Comment 24 by amyressler@google.com on Fri, Apr 15, 2022, 9:58 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:09 PM EDT Project Member

Labels: Release-0-M101

Comment 26 by amyressler@google.com on Tue, Apr 26, 2022, 4:31 PM EDT Project Member

Labels: CVE-2022-1488 CVE_description-missing

Comment 27 by rzanoni@google.com on Tue, Jul 5, 2022, 3:28 AM EDT Project Member

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 28 by sheriffbot on Tue, Jul 5, 2022, 3:32 AM EDT Project Member

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

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 29 by rzanoni@google.com on Tue, Jul 5, 2022, 3:40 AM EDT Project Member

1. Just https://crrev.com/c/3736386
2. Medium, a few datatype and missing methods conflicts.
3. Merged into main on Mar 26
4. Yes

Comment 30 by gmpritchard@google.com on Wed, Jul 6, 2022, 10:41 AM EDT Project Member

Labels: -LTS-Merge-Candidate

@rzanoni, if conflicts were resolved, I'll approve.

Comment 31 by gmpritchard@google.com on Wed, Jul 6, 2022, 10:51 AM EDT Project Member

Labels: LTS-Merge-Approved-96

Comment 32 by gmpritchard@google.com on Wed, Jul 6, 2022, 1:23 PM EDT Project Member

Labels: -LTS-Merge-Review-96

Comment 33 by Git Watcher on Thu, Jul 7, 2022, 8:21 AM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/8f85e66ea4dda915705243d0c8d97906143e4253

commit 8f85e66ea4dda915705243d0c8d97906143e4253
Author: Istiaque Ahmed <lazyboy@chromium.org>
Date: Thu Jul 07 12:20:25 2022

[M96-LTS][Extensions] Fix inadvertent leakage of info through event listeners.

M96 merge issues:
tabs_event_router.cc:
- M96 uses event_args->Set instead of Append on WillDispatchTabUpdatedEvent
and tab_value->SetBoolean instead of SetBoolKey on WillDispatchTabCreatedEvent

windows_event_router.cc:
- multiple conflicts because has_window_exposed_by_default is not present in M96
- filter_info init conflicts

extension_tabs_apitest.cc:
- SendMessage not present in M96

event_router.cc:
- event->filter_info is not cloned in M96

Different extension event implementations (e.g. tabs.onCreated) can
tweak their listener params through Event::WillDispatchCallback
callback. It does so by passing mutable Event* to
WillDispatchCallback. This can lead to one extension's
event listener inadvertently affecting a different extension's
event listener, as the (modified) `Event*` is carried over to
next/subsequent listeners.

This CL changes this by removing the mutable Event param from
WillDispatchCallback, and exposes "writable" `event_args_out`
and `event_filtering_info_out` params to WillDispatchCallback. This
is done so that interested parties can set those modified params
to be used by dispatcher (EventRouter::DispatchExtensionMessage).

Note that events funneled through LazyEventDispatcher is not
currently susceptible to this problem as it copies Event-s before
dispatching them.

(cherry picked from commit 940ddcfaff7bca60f7df77e54735c4f808933bfa)

~~Bug: 1302959~~
Change-Id: I1fbb9b9b29ff2f05c620f2a64f875d83db472136
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3531082
Commit-Queue: Istiaque Ahmed <lazyboy@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#985564}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3736286

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3736386
Owners-Override: Michael Ershov <miersh@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Reviewed-by: Michael Ershov <miersh@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1658}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/chrome/browser/extensions/api/tabs/windows_event_router.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/api/audio/audio_api.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/event_router.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/api/usb/usb_device_manager.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/events/lazy_event_dispatcher.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/api/printer_provider/printer_provider_api.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/chrome/browser/extensions/api/downloads/downloads_api.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/event_router.h
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/chrome/browser/extensions/api/tabs/tabs_event_router.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/extensions/browser/api/hid/hid_device_manager.cc
[modify] https://crrev.com/8f85e66ea4dda915705243d0c8d97906143e4253/chrome/browser/extensions/extension_tabs_apitest.cc

Comment 34 by rzanoni@google.com on Thu, Jul 7, 2022, 8:22 AM EDT Project Member

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 35 by sheriffbot on Sat, Jul 9, 2022, 1:31 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 36 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 37 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing