Starred by 2 users

Owner:	rdevl...@chromium.org
CC:	lazyboy@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2022-01-24
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

reward-5000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
M-98
Target-98
FoundIn-96
Security_Impact-Extended
LTS-NotApplicable-96
Release-0-M100
CVE-2022-1137

Issue 1289846: Security: CSS keylogger extension using PageStateMatcher and chrome.action.openPopup()

Reported by stw.s...@gmail.com on Fri, Jan 21, 2022, 5:36 PM EST

Code

VULNERABILITY DETAILS

An extension without the permission to read the page's content can exfiltrate sensitive values using DeclarativeContent CSS selectors and chrome.action.openPopup().

VERSION

Chrome Version: 99.0.4844.0 + dev
Operating System: Windows 10

REPRODUCTION CASE

1. Install the extension and open the target page.
2. You will find the exfiltrated password value in the extension console.

chrome.declarativeContent API [0] allows to enable the extension action popup based on a CSS selector on the focused page.

First, we disable the action popup.

```
chrome.action.disable();
```

This code will enable the popup only if the current page has an iframe matching the specified selector.

```
chrome.declarativeContent.onPageChanged.addRules([{
  conditions: [
    new chrome.declarativeContent.PageStateMatcher({
      pageUrl: { hostEquals: 'example.com', schemes: ['https'] },
      css: ['iframe[src^="https://example.com/?access_key=a"]']
    }),
  ], actions: [
    new chrome.declarativeContent.ShowAction(),
  ]
}]);
```

If we try to open the popup programmatically [1] and it fails with an error, it means the selector did not match. If no error is thrown, the selector was matched.

```
try {
  await chrome.action.openPopup();
} catch (e) {
  error = true;
}
```

Now, we can use binary search to quickly find the exact value of the attribute. In my testing, 50 queries per second works reliably.

We can use this technique to extract input values/passwords*, leak access tokens from iframes and other sensitive data.

* By default, CSS selectors won't match [value=...] attributes [2], but libraries like React set the value attribute directly on the element, making this attack feasible on a large number of websites.

CREDIT INFORMATION
Reporter credit: Thomas Orlita

[0]: https://developer.chrome.com/docs/extensions/reference/declarativeContent
[1]: https://developer.chrome.com/docs/extensions/reference/action/#method-openPopup
[2]: https://css-tricks.com/css-keylogger/

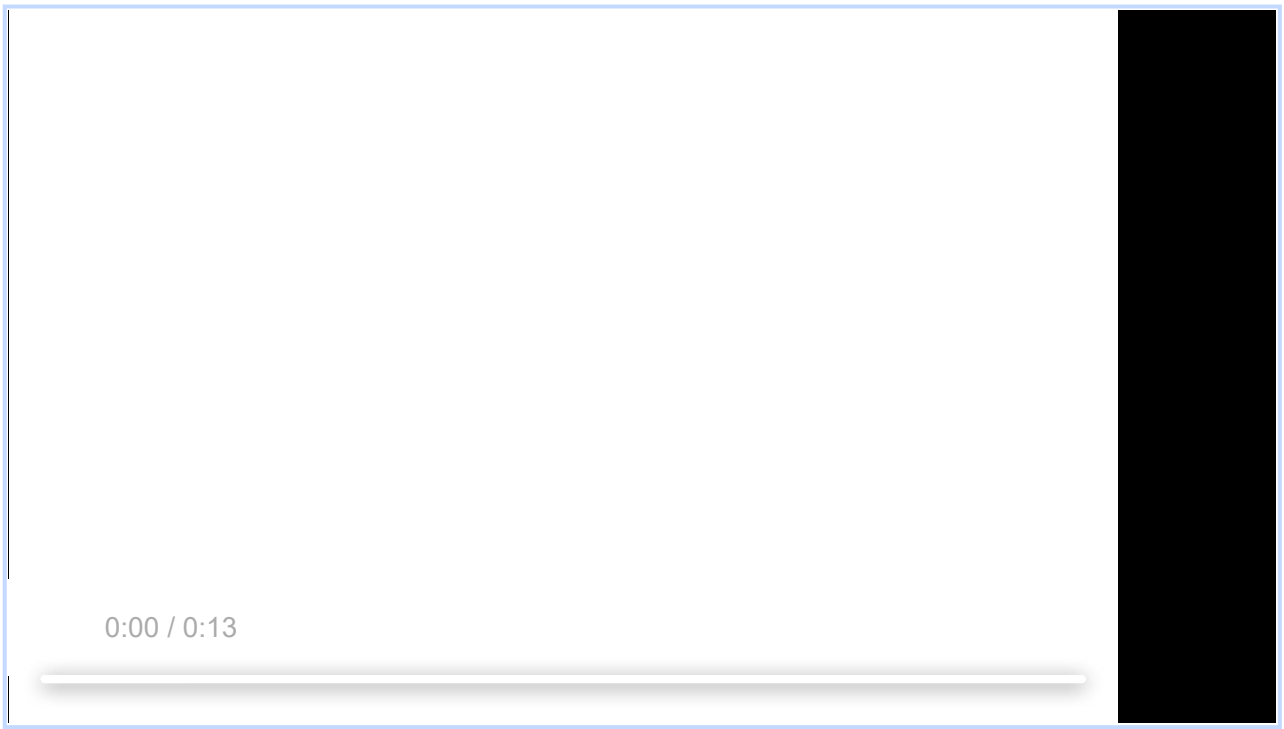
background.js
2.0 KB View Download

manifest.json
292 bytes View Download

popup.html
32 bytes View Download

popup.js
15 bytes View Download

poc.mp4
556 KB View Download



Comment 1 by sheriffbot on Fri, Jan 21, 2022, 5:45 PM EST Project Member

Labels: external_security_report

Comment 2 by ajgo@google.com on Fri, Jan 21, 2022, 6:15 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: rdevl...@chromium.org
Cc: lazyboy@chromium.org
Labels: Security_Severity-Medium FoundIn-96 OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros
Components: Platform>Extensions

Hi Devlin could you take a look at this one there is a good video and poc. This might be a privacy issue, but I feel it is also a permissions bypass for extensions.

Comment 3 by sheriffbot on Fri, Jan 21, 2022, 6:15 PM EST Project Member

Labels: Security_Impact-Extended

Comment 4 by rdevl...@chromium.org on Fri, Jan 21, 2022, 7:04 PM EST Project Member

Labels: Pri-1
NextAction: 2022-01-24

Oh, that's cool! Great find!

Luckily, this API is still restricted to dev channel [1], so this won't reproduce on stable. But definitely something we should fix. I think a fairly straightforward solution would be to not consider a declaratively-visible popup for the API. I'll see if I can do that next week.

[1] https://source.chromium.org/chromium/chromium/src/+/main:chrome/common/extensions/api/_api_features.json;l=66;drc=f568aedcc729dbe7746eebe57a1723ae0760220b

Comment 5 by sheriffbot on Sat, Jan 22, 2022, 12:52 PM EST Project Member

Labels: M-98 Target-98

Setting milestone and target because of medium severity.

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

Comment 6 by monor...@bugs.chromium.org on Mon, Jan 24, 2022, 7:00 AM EST

The NextAction date has arrived: 2022-01-24

Comment 7 by Git Watcher on Thu, Jan 27, 2022, 12:40 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b

commit 6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b
Author: Devlin Cronin <rdevlin.cronin@chromium.org>
Date: Thu Jan 27 17:38:57 2022

[Extensions] Don't allow opening a popup for a declarative-shown action

Actions can be declaratively shown using the chrome.declarativeContent API, where they can be active on a tab for certain CSS selectors. This information should not be returned to the extension, since it can leak information about the page.

The action.openPopup() (and browserAction.openPopup()) API will open a popup on a given tab if the action is visible on the tab, and will

popup on a given tab if the action is visible on the tab, and will otherwise fail and return an error. Adjust this so that the API doesn't include declarative action shows so that extensions can't indirectly retrieve this information.

Adjust this for both APIs (action.openPopup() and browserAction.openPopup()), and add a regression test.

~~Bug: 1289846~~
Change-Id: Ib9ea8b5474df2222287b972db7dbfe97d46dcbbc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3413808
Reviewed-by: David Bertoni <dbertoni@chromium.org>
Commit-Queue: Devlin Cronin <rdevlin.cronin@chromium.org>
Cr-Commit-Position: refs/heads/main@{#964109}

[modify] https://crrev.com/6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b/extensions/browser/extension_action.cc
[modify] https://crrev.com/6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b/extensions/browser/extension_action_unittest.cc
[modify] https://crrev.com/6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b/chrome/browser/extensions/api/extension_action/extension_action_api.cc
[modify] https://crrev.com/6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b/extensions/browser/extension_action.h
[modify] https://crrev.com/6f1205eddca62b071cc2ca2ed5d82d7fc1b5a89b/chrome/browser/extensions/api/extension_action/extension_action_api_interactive_uitest.cc

Comment 8 by rdevl...@chromium.org on Thu, Jan 27, 2022, 1:52 PM EST Project Member

Status: Fixed (was: Assigned)

This should be fixed.

Since the API is restricted to dev channel, this probably doesn't need a merge (even though the original change landed in M99 and the fix was in M100). I'd also lean towards downgrading the severity to "low" since a) this requires extension installation and b) it requires dev channel, but I'll leave that to the security folks. :)

Thank you again for the report!

Comment 9 by sheriffbot on Fri, Jan 28, 2022, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 10 by sheriffbot on Fri, Jan 28, 2022, 1:41 PM EST Project Member

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

Comment 11 by sheriffbot on Fri, Jan 28, 2022, 2:12 PM EST Project Member

Labels: Merge-Request-98 Merge-Request-99

Requesting merge to beta M98 because latest trunk commit (964109) appears to be after beta branch point (950365).

Requesting merge to dev M99 because latest trunk commit (964109) appears to be after dev branch point (961656).

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

Comment 12 by sheriffbot on Fri, Jan 28, 2022, 2:14 PM EST Project Member

Labels: -Merge-Request-99 Hotlist-Merge-Approved Merge-Approved-99

Merge approved: your change passed merge requirements and is auto-approved for M99. Please go ahead and merge the CL to branch 4844 (refs/branch-heads/4844) 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: benmason (Android), harrysouders (iOS), cindyb (ChromeOS), pbommana (Desktop)

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

Comment 13 by sheriffbot on Fri, Jan 28, 2022, 2:14 PM EST Project Member

Labels: -Merge-Request-98 Merge-Review-98 Hotlist-Merge-Review

Merge review required: M98 has already been cut for stable release.

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

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

Comment 14 by rdevl...@chromium.org on Fri, Jan 28, 2022, 5:15 PM EST Project Member

Labels: -Hotlist-Merge-Review -Hotlist-Merge-Approved -M-98 -Merge-Approved-99 -Target-98 -Merge-Review-98

Wow, sheriffbot has been having a very interesting conversation with itself! ;)

I think there's no need for a merge here. See comment c#8:

> Since the API is restricted to dev channel, this probably doesn't need a merge

Comment 15 by sheriffbot on Sun, Jan 30, 2022, 12:51 PM EST Project Member

Labels: M-98 Target-98

Setting milestone and target because of medium severity.

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

Comment 16 by amyressler@google.com on Thu, Mar 3, 2022, 5:23 PM EST 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

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 17 by amyressler@chromium.org on Thu, Mar 3, 2022, 5:51 PM EST Project Member

Congratulations, Thomas! The VRP Panel has decided to award you $5,000 for this report. Thank you for your efforts and good work!

Comment 18 by amyressler@google.com on Fri, Mar 4, 2022, 6:34 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 19 by amyressler@chromium.org on Mon, Mar 28, 2022, 6:00 PM EDT Project Member

Labels: Release-0-M100

Comment 20 by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT Project Member

Labels: CVE-2022-1137 CVE_description-missing

Comment 21 by gmpritchard@google.com on Thu, Mar 31, 2022, 12:04 PM EDT Project Member

Labels: LTS-NotApplicable-96

Not Applicable to LTS-96 per Comment#4

Comment 22 by sheriffbot on Fri, May 6, 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 23 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 24 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing