☆ Starred by 2 users

Owner:	nicolaso@chromium.org
CC:	pastarmovj@chromium.org
Status:	Fixed *(Closed)*
Components:	Enterprise>BrowserSwitcher
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

reward-2000
Security_Severity-Medium
Arch-x86_64
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
M-99
Target-99
FoundIn-98
Security_Impact-Extended
Release-0-M101
CVE-2022-1490

Issue 1301840: uaf in browser_switcher::`anonymous namespace'::OpenBrowserSwitchPage

Reported by wxhu...@gmail.com on Mon, Feb 28, 2022, 8:34 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

Steps to reproduce the problem:
1.I patch the chromium to easy enter the code path
2. open chromium. it will Open 'chrome://browser-switch/?url=...' in the current tab.
3.then close the current tab

What is the expected behavior?

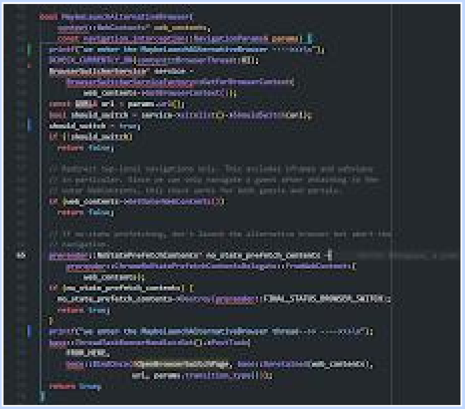
What went wrong?
uaf occur

Did this work before? N/A

Chrome version: 98.0.4758.102 Channel: stable
OS Version: 10.0

asan.txt
17.4 KB View Download

issue_poc.png
67.0 KB View Download



```
bool MaybeLaunchAlternativeBrowser(
    content::WebContents* web_contents,
    const navigation_interception::NavigationParams& params) {
  printf("we enter the MaybeLaunchAlternativeBrowser ---->\n");
  DCHECK_CURRENTLY_ON(content::BrowserThread::UI);
  BrowserSwitcherService* service =
      BrowserSwitcherServiceFactory::GetForBrowserContext(
          web_contents->GetBrowserContext());
  const GURL& url = params.url();
  bool should_switch = service->sitelist()->ShouldSwitch(url);
  should_switch = true;
  if (!should_switch)
    return false;

  // Redirect top-level navigations only. This excludes iframes and webviews
  // in particular. Since we can only navigate a guest after attaching to the
  // outer WebContents, this check works for both guests and portals.
  if (web_contents->GetOuterWebContents())
    return false;

  // If no-state prefetching, don't launch the alternative browser but abort the
  // navigation.
  prerender::NoStatePrefetchContents* no_state_prefetch_contents =
      prerender::ChromeNoStatePrefetchContentsDelegate::FromWebContents(
          web_contents);
  if (no_state_prefetch_contents) {
    no_state_prefetch_contents->Destroy(prerender::FINAL_STATUS_BROWSER_SWITCH);
    return true;
  }
  printf("we enter the MaybeLaunchAlternativeBrowser thread--> ---->\n");
  base::ThreadTaskRunnerHandle::Get()->PostTask(
      FROM_HERE,
      base::BindOnce(&OpenBrowserSwitchPage, base::Unretained(web_contents),
                     url, params.transition_type()));
  return true;
}
```

Comment 1 by sheriffbot on Mon, Feb 28, 2022, 8:40 PM EST

Labels: external_security_report

Comment 2 Deleted

Comment 3 by wxhu...@gmail.com on Mon, Feb 28, 2022, 8:44 PM EST

you can set owner to nicolaso@chromium.org.
how to fix
- set web_contents to weak_ptr

- set web_contents to weak_ptr

Comment 4 by wxhu...@gmail.com on Mon, Feb 28, 2022, 9:04 PM EST

my chromium commit is 1648616c1dafa4d3624552c2ce282be5129290db

Comment 5 Deleted

Comment 6 by wxhu...@gmail.com on Tue, Mar 1, 2022, 3:30 AM EST

0001-fix-issue-1301840-uaf.patch
2.0 KB View Download

Comment 7 by amyressler@chromium.org on Tue, Mar 1, 2022, 3:14 PM EST

Cc: nicolaso@chromium.org
Labels: FoundIn-98 Security_Severity-Medium
Components: Enterprise>BrowserSwitcher

I have not reproduced this, tentatively setting this as medium severity based on POC and that the patch being introduced seems to be a requirement to trigger; over to you nicolaso@ as requested

Comment 8 by sheriffbot on Tue, Mar 1, 2022, 3:20 PM EST

Labels: Security_Impact-Extended

Comment 9 by nicolaso@chromium.org on Wed, Mar 2, 2022, 10:41 AM EST

Hm, this doesn't repro locally on Windows. wxhusst@, what's the contents of your args.gn? Maybe something in there is making it easier to trigger.

IIUC, your patch only adds logging, and sets should_switch=true.

>the patch being introduced seems to be a requirement to trigger

It's not a requirement, but I suspect it's *very* hard (impossible?) to trigger in an official build. What the patch does is "force all navigations to trigger BrowserSwitcher".

BrowserSwitcher is a feature hidden behind an enterprise policy (which only has ~8M 30DAUs). It sets a list of URLs (typically a small number of websites) that will trigger this particular code path. It's also a *really* tight race condition, at least without the patch.

More importantly, this seems to depend on certain build-time arguments. Even on an asan build, I can't seem to repro this bug...

Comment 10 by nicolaso@chromium.org on Wed, Mar 2, 2022, 10:50 AM EST

Status: Started (was: Unconfirmed)
Owner: nicolaso@chromium.org
Cc: -nicolaso@chromium.org

In short, I don't know whether this actually repros in the wild/has a security impact.

It's an easy fix though. Using a WeakPtr is the correct thing to do, so let me work on that

Comment 11 by nicolaso@chromium.org on Wed, Mar 2, 2022, 11:07 AM EST

Cc: pastarmovj@chromium.org

Comment 12 by Git Watcher on Wed, Mar 2, 2022, 12:48 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e7e87d05d58bc70611401f655dc845498357f8e4

commit e7e87d05d58bc70611401f655dc845498357f8e4
Author: Nicolas Ouellet-Payeur <nicolaso@chromium.org>
Date: Wed Mar 02 17:47:01 2022

[BrowserSwitcher] Use a WeakPtr in the NavigationThrottle

When calling OpenBrowserSwitchPage(), we passed the WebContents by
raw pointer rather than a WeakPtr. It was posted to a task, so that
can be unsafe.

~~Bug: 1301840~~
Change-Id: I42e1daaf0773d08251000770e65c5d8674867921
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3498165
Commit-Queue: Nicolas Ouellet-Payeur <nicolaso@chromium.org>
Auto-Submit: Nicolas Ouellet-Payeur <nicolaso@chromium.org>
Reviewed-by: Julian Pastarmov <pastarmovj@chromium.org>
Commit-Queue: Julian Pastarmov <pastarmovj@chromium.org>
Cr-Commit-Position: refs/heads/main@{#976720}

[modify]
https://crrev.com/e7e87d05d58bc70611401f655dc845498357f8e4/chrome/browser/browser_switcher/browser_switcher_navigation_throttle.cc

Comment 13 by sheriffbot on Wed, Mar 2, 2022, 12:52 PM EST

Labels: M-99 Target-99

Setting milestone and target because of medium severity.

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

Comment 14 by sheriffbot on Wed, Mar 2, 2022, 1:18 PM EST

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 15 by wxhu...@gmail.com on Wed, Mar 2, 2022, 5:00 PM EST

this is my contents of args.gn, I just patch chrome/browser/browser_switcher/browser_switcher_navigation_throttle.cc

```
# Build arguments go here.
# See "gn args <out_dir> --list" for available build arguments.
is_debug =false
is_asan = true


dcheck_always_on = false
enable_mojom_fuzzer = true
```

Comment 16 by wxhu...@gmail.com on Wed, Mar 2, 2022, 5:05 PM EST

>BrowserSwitcher is a feature hidden behind an enterprise policy (which only has ~8M 30DAUs). It sets a list of URLs (typically a small number of websites) that will trigger this particular code path. It's also a *really* tight race condition, at least without the patch.

could the list of URLs set to "chrome://browser-switch/*" ? If it can, I think the bug can be triggered easily , because all navigations will enter into "chrome://browser-switch/" and always reload.

Comment 17 by nicolaso@chromium.org on Wed, Mar 2, 2022, 5:06 PM EST

> could the list of URLs set to "chrome://browser-switch/*" ?

No. Only http://, https://, and ftp:// URLs are allowed

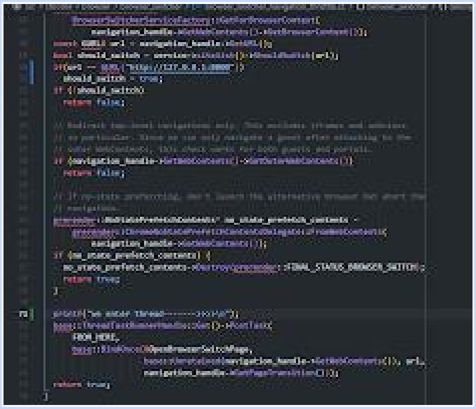
Comment 18 by wxhu...@gmail.com on Wed, Mar 2, 2022, 5:09 PM EST

oh, it seems a tight race condition in real chrome

Comment 19 by wxhu...@gmail.com on Wed, Mar 2, 2022, 5:30 PM EST

oh, I can trigger it stable,
- set a url to switch
- open test.html
- then close chrome

poc1.png
92.0 KB View Download

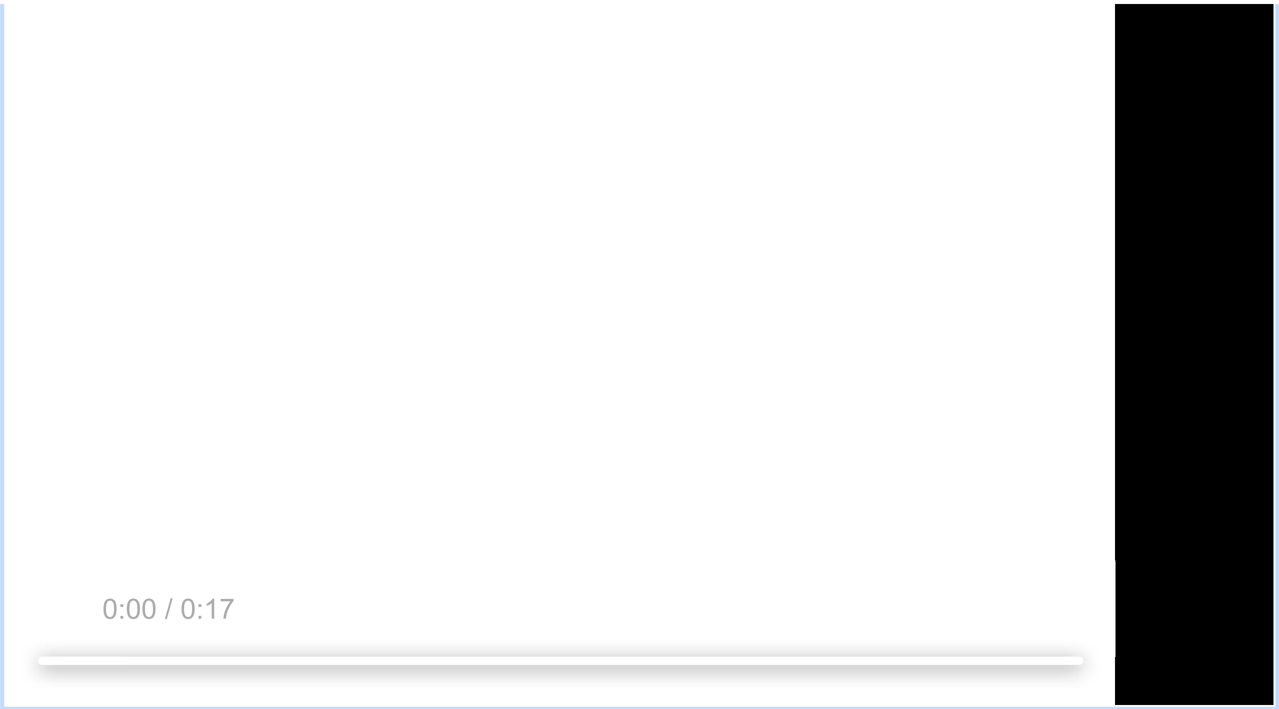


```
      BrowserSwitcherServiceFactory::GetForBrowserContext(
          navigation_handle->GetWebContents()->GetBrowserContext());
  const GURL& url = navigation_handle->GetURL();
  bool should_switch = service->sitelist()->ShouldSwitch(url);
  if(url == GURL("http://127.0.0.1:8000"))
    should_switch = true;
  if (!should_switch)
    return false;

  // Redirect top-level navigations only. This excludes iframes and webviews
  // in particular. Since we can only navigate a guest after attaching to the
  // outer WebContents, this check works for both guests and portals.
  if (navigation_handle->GetWebContents()->GetOuterWebContents())
    return false;

  // If no-state prefetching, don't launch the alternative browser but abort the
  // navigation.
  prerender::NoStatePrefetchContents* no_state_prefetch_contents =
      prerender::ChromeNoStatePrefetchContentsDelegate::FromWebContents(
          navigation_handle->GetWebContents());
  if (no_state_prefetch_contents) {
    no_state_prefetch_contents->Destroy(prerender::FINAL_STATUS_BROWSER_SWITCH);
    return true;
  }

  printf("we enter thread------->>>\n");
  base::ThreadTaskRunnerHandle::Get()->PostTask(
      FROM_HERE,
      base::BindOnce(&OpenBrowserSwitchPage,
                     base::Unretained(navigation_handle->GetWebContents()), url,
                     navigation_handle->GetPageTransition()));
  return true;
}
```

test.html
172 bytes View Download

poc1.mp4
8.2 MB View Download

[redacted]



Comment 20 by wxhu...@gmail.com on Wed, Mar 2, 2022, 5:32 PM EST

I think this bug should set Security_Severity-High

Comment 21 by wxhu...@gmail.com on Wed, Mar 2, 2022, 5:42 PM EST

hello, nicolaso, I think we can set the bug to fixed.

Comment 22 by nicolaso@chromium.org on Thu, Mar 3, 2022, 1:45 PM EST

Status: Fixed (was: Started)

Correct, it's Fixed by crrev.com/c/3498165

test.html in Comment #19 is important, as it shows how an attacker could try to exploit this vulnerability.

There's a few mitigating factors:
- Requires the BrowserSwitcherEnabled policy to be set. (relatively low usage, ~8M DAUs)
- The attacker needs to know (or guess!) the contents of the BrowserSwitcherUrlList policy, in order to know what JavaScript to "inject".
- The user has to click the "X" button to trigger the UaF.
    - ... but they're pretty likely to do that, if Chrome is freezing because of 100+ tabs opening suddenly.
    - ... and if the attacker is running their JS in a malicious extension, they can close all windows via JavaScript.

Anyways, if all those conditions are fulfilled it's a pretty big deal. I'll let the security team make the final call RE: severity, but it seems rather high.

Comment 23 by nicolaso@chromium.org on Fri, Mar 4, 2022, 9:53 AM EST

Actually combing through Severity Guidelines for the firs time [1] I would be tempted to leave it as Medium severity.

> Bugs that would normally be rated at a higher severity level with unusual mitigating factors may be rated as medium severity.

Again, this requires the attacker to know the policy's value, and that they already have a malicious extension on the user's machine (or control an origin in that list, in which case it requires user interaction).

machine (or control an origin in that list, in which case it requires user interaction).

And it only affects users with the BrowserSwitcherEnabled policy, which has low usage; but IIUC this is not a big mitigating factor:

> Conversely, we do not consider it a mitigating factor if a vulnerability applies only to a particular group of users. For instance, a Critical vulnerability is still considered Critical even if it applies only to Linux or to those users running with accessibility features enabled.

Anyways, Medium seems more appropriate based on the examples on that page.

[1] https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/severity-guidelines.md

Comment 24 by sheriffbot on Fri, Mar 4, 2022, 12:42 PM EST

Labels: reward-topanel

Comment 25 by sheriffbot on Fri, Mar 4, 2022, 1:41 PM EST

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

Comment 26 by amyressler@google.com on Thu, Mar 10, 2022, 10:40 PM EST

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 27 by amyressler@chromium.org on Thu, Mar 10, 2022, 11:36 PM EST

Congratulations, raven! The VRP Panel has decided to award you $2,000 for this report.
This report was judged under the updated VRP rules and policies related to bugs requiring complex user interaction. [1] We appreciate your efforts and reporting this issue to us!

[1] https://g.co/chrome/vrp

Comment 28 by amyressler@google.com on Fri, Mar 11, 2022, 2:42 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 29 by wxhu...@gmail.com on Fri, Mar 11, 2022, 9:38 PM EST

hi amy, I don't think this bug need complex user interaction.You can see the step of comment 22. Hope you can recheck it. Can this bug get cve id?

Comment 30 by wxhu...@gmail.com on Fri, Mar 11, 2022, 9:47 PM EST

as [1] shows that the suggest patch can get additional rewards, can my patch in [2] get the additional rewards?

[1] https://g.co/chrome/vrp
[2] https://bugs.chromium.org/p/chromium/issues/detail?id=1301840#c6

Comment 31 by amyressler@chromium.org on Mon, Mar 14, 2022, 5:07 PM EDT

Hi raven, thanks for your questions in comments 29-30:

>> I don't think this bug need complex user interaction.You can see the step of comment 22.

In comment 22-23, the developer lists the number of mitigations, which are significant and also concurs with the severity and impact (in comment #23)
The VRP Panel took all of this into consideration when making the reward decision.

>>Can this bug get cve id?
As always, CVEs are allocated when the patch is shipped in a stable channel release. One will be allocated to this bug report once this patch is included in the a stable release candidate.

>>as [1] shows that the suggest patch can get additional rewards, can my patch in [2] get the additional rewards?
while it does not appear we used your patch in full, we will reassess the potential patch reward at the next panel

Comment 32 by wxhu...@gmail.com on Mon, Mar 14, 2022, 7:26 PM EDT

Ok, thank you

Comment 33 by amyressler@chromium.org on Wed, Mar 16, 2022, 7:21 PM EDT

hello raven, the VRP panel has reviewed this issue for reassessment and has decided that the original award amount was sufficient for this report.

Comment 34 by wxhu...@gmail.com on Wed, Mar 16, 2022, 7:32 PM EDT

Thanks a lot 👍

Comment 35 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:10 PM EDT

Labels: Release-0-M101

Comment 36 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT

Labels: CVE-2022-1490 CVE_description-missing

Comment 37 by sheriffbot on Fri, Jun 10, 2022, 1:31 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

Comment 38 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 39 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing