


☆ Starred by 3 users

**Owner:** [peter@chromium.org](mailto:peter@chromium.org)

**CC:** [dominickn@chromium.org](mailto:dominickn@chromium.org)  
[engedy@chromium.org](mailto:engedy@chromium.org)  
[msramek@chromium.org](mailto:msramek@chromium.org)  
 [hkamila@chromium.org](mailto:hkamila@chromium.org)  
[peter@chromium.org](mailto:peter@chromium.org)

**Status:** Fixed (Closed)

**Components:** [UI>Notifications](#)  
[UI>Browser>Permissions>Prompts](#)

**Modified:** Jan 8, 2021

**Backlog-Rank:** ---

**Editors:** ---

**EstimatedDays:** ---

**NextAction:** ---

**OS:** [Linux](#)

**Pri:** [2](#)

**Type:** [Bug-Security](#)

[reward-500](#)  
[Security\\_Severity-Low](#)  
[Security\\_Impact-Stable](#)  
[allpublic](#)  
[reward-inprocess](#)  
[Via-Wizard-Security](#)  
[CVE\\_description-submitted](#)  
[Target-72](#)  
[Target-73](#)  
[Target-74](#)  
[Target-75](#)  
[Target-76](#)  
[Target-77](#)  
[Target-78](#)  
[Hotlist-Permissions](#)  
[M-78](#)  
[Release-0-M74](#)  
[CVE-2020-6504](#)

**Issue 875503: Chrome notification system permits to a domain to request permissions for each 3rd level domain with no restriction**  
Reported by [aless...@gmail.com](mailto:aless...@gmail.com) on Fri, Aug 17, 2018, 7:16 PM EDT

 Code

UserAgent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36

Steps to reproduce the problem:  
1. Go to this link <https://ovx5b.browsersecurely.com/index2.php?t=90&c=11&hash=5241408335b72b23&subid=52ed9gXuqoja23y801&url=https%3A%2F%2Ftraliapon.tk%2Fclick.php%3Fkey%3Df8oncxh3s3cbfks02fr&=714671>  
2. Deny the consent to notification  
3. Loop

What is the expected behavior?  
Request stop after some redirects.

What went wrong?  
The website ask to the user infinite amount of time the notification permission

Did this work before? N/A

Chrome version: 68.0.3440.84 Channel: stable  
OS Version:  
Flash Version:

See the source of the html file  
Regards

**chrome\_exploit.html**  
27.6 KB [View](#) [Download](#)

[Comment 1](#) by [carlosil@chromium.org](mailto:carlosil@chromium.org) on Fri, Aug 17, 2018, 8:16 PM EDT Project Member

**Status:** Assigned (was: Unconfirmed)  
**Owner:** [peter@chromium.org](mailto:peter@chromium.org)  
**Labels:** [Security\\_Severity-Low](#)  
**Components:** [UI>Notifications](#)

peter: Looks like this allows sites to ask for notification permission endless times, can you take a look?

In my opinion this wouldn't be a security bug (merely an annoyance), but keeping it as a low severity one just in case.

[Comment 2](#) by [tsepez@chromium.org](mailto:tsepez@chromium.org) on Tue, Aug 28, 2018, 1:54 PM EDT Project Member

**Labels:** [Security\\_Impact-Stable](#)

[Comment 3](#) by [peter@chromium.org](mailto:peter@chromium.org) on Tue, Aug 28, 2018, 1:56 PM EDT Project Member

**Cc:** [dominickn@chromium.org](mailto:dominickn@chromium.org)

+Dominick for his opinion.

We're looking at requiring a user gesture for requesting notification permission, but other than that there's not a whole lot here that's immediately actionable...

[Comment 4](#) by [dominickn@chromium.org](mailto:dominickn@chromium.org) on Tue, Aug 28, 2018, 6:59 PM EDT Project Member

Cc: [msramek@chromium.org](mailto:msramek@chromium.org) [engedy@chromium.org](mailto:engedy@chromium.org) [hkamila@chromium.org](mailto:hkamila@chromium.org)

**Components:** UI>Browser>Permissions>Prompts

Yeah, this is a notable crack in the web's permission model - that you can just redirect to different origins and request again. We'll need to make platform breaking changes (like requiring a gesture) , or do an browser intervention (e.g. throttle permission requests to N per minute) to address it.

Users should always be able to close the tab and leave the loop, making this less serious (though it's more annoying on Android where the permission prompt is modal).

+ some other permissions folks. The idea of throttling permission requests through the PermissionRequestManager has come up before and might be a good way to tackle this. We could simply rate-limit the number of requests that can be made per some time frame. If we want to be fancier, we can rate-limit per origin or per ETLD+1, but a global limit seems simpler - even having something like limiting to 1 request of the same permission per 10 seconds might be enough to take the teeth out of this sort of abusive site.

[Comment 5](#) by [tsepez@chromium.org](mailto:tsepez@chromium.org) on Wed, Aug 29, 2018, 1:42 PM EDT Project Member

**Labels:** M-70

[Comment 6](#) by [engedy@chromium.org](mailto:engedy@chromium.org) on Tue, Sep 4, 2018, 7:12 AM EDT Project Member

**Labels:** -M-70 Hotlist-Permissions M-71

[Comment 7](#) by [mbarb...@chromium.org](mailto:mbarb...@chromium.org) on Mon, Sep 24, 2018, 12:21 PM EDT Project Member

[Issue 888210](#) has been merged into this issue.

[Comment 8](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Jan 30, 2019, 9:01 AM EST Project Member

**Labels:** -M-71 Target-72 M-72

[Comment 9](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Mar 13, 2019, 9:01 AM EDT Project Member

**Labels:** -M-72 Target-73 M-73

[Comment 10](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Apr 24, 2019, 9:02 AM EDT Project Member

**Labels:** -M-73 Target-74 M-74

[Comment 11](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Jun 5, 2019, 9:02 AM EDT Project Member

**Labels:** -M-74 M-75 Target-75

[Comment 12](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Jul 31, 2019, 9:03 AM EDT Project Member

**Labels:** -M-75 M-76 Target-76

[Comment 13](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Sep 11, 2019, 9:05 AM EDT Project Member

**Labels:** -M-76 M-77 Target-77

[Comment 14](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Oct 23, 2019, 9:14 AM EDT Project Member

**Labels:** -M-77 Target-78 M-78

[Comment 15](#) by [peter@chromium.org](mailto:peter@chromium.org) on Fri, Dec 6, 2019, 10:21 AM EST Project Member

I'm going to close this as Fixed - the Reparo team introduced a restriction in M76 (IIRC) where this flow becomes infeasible: permission requests will be placed under embargo after the third dismissed request.

[Comment 16](#) by [peter@chromium.org](mailto:peter@chromium.org) on Fri, Dec 6, 2019, 10:45 AM EST Project Member

**Status:** Fixed (was: Assigned)

[Comment 17](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Sat, Dec 7, 2019, 10:46 AM EST Project Member

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

[Comment 18](#) by [awhalley@chromium.org](mailto:awhalley@chromium.org) on Wed, Dec 11, 2019, 5:53 PM EST Project Member

**Labels:** reward-topanel

[Comment 19](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, Dec 19, 2019, 12:34 PM EST Project Member

**Labels:** -reward-topanel reward-unpaid reward-500

\*\*\* 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](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

[Comment 20](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, Dec 19, 2019, 12:39 PM EST Project Member

Congrats! The Panel decided to reward \$500 for this report!

[Comment 21](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, Dec 19, 2019, 12:47 PM EST Project Member

**Labels:** -reward-unpaid reward-inprocess

[Comment 22](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Thu, Jan 30, 2020, 6:33 PM EST Project Member

[peter@chromium.org](mailto:peter@chromium.org) - with regards to [#c15](#), was that change in the initial M76 release? (I assume so, as opposed to in some subsequent respin). We'll need to allocate a CVE for this and amend the relevant release notes to credit this reporter. If you can provide a crbug number for the Reparo change that'd be great, but no worries if not.

[Comment 23](#) by [peter@chromium.org](mailto:peter@chromium.org) on Fri, Jan 31, 2020, 6:48 AM EST Project Member

engedy@ - do you have that information handy?

[Comment 24](#) by [engedy@chromium.org](mailto:engedy@chromium.org) on Thu, Feb 20, 2020, 1:14 PM EST Project Member

The mitigation is tracked in [crbug.com/900000](https://crbug.com/900000). It was merged back to 74.0.3729.91. According to [1], the initial M74 release was a later revision than this.

[1]: [https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop\\_23.html](https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_23.html)

Comment 25 by [adetaylor@google.com](mailto:adetaylor@google.com) on Mon, Mar 9, 2020, 2:41 PM EDT Project Member

**Labels:** Release-0-M74

Thanks.

Comment 26 by [sheriffbot](#) on Fri, Mar 13, 2020, 1:59 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 27 by [adetaylor@google.com](mailto:adetaylor@google.com) on Mon, Jun 1, 2020, 5:13 PM EDT Project Member

**Labels:** relnotes\_update\_needed

Comment 28 by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Jun 3, 2020, 12:56 PM EDT Project Member

[alessio.dimaria@gmail.com](mailto:alessio.dimaria@gmail.com), how would you like to be credited in the release notes here? Sorry for the delay in getting this properly credited!

Comment 29 by [aless...@gmail.com](mailto:aless...@gmail.com) on Wed, Jun 3, 2020, 4:57 PM EDT

you can put my full name: Alessio Di Maria

regards

Comment 30 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Wed, Jun 3, 2020, 5:47 PM EDT Project Member

**Labels:** CVE-2020-6504 CVE\_description-missing

Comment 31 by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Jun 3, 2020, 5:57 PM EDT Project Member

Thanks, will do.

Comment 32 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Wed, Jun 3, 2020, 7:11 PM EDT Project Member

**Labels:** -CVE\_description-missing CVE\_description-submitted

Comment 33 by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, Jan 8, 2021, 5:38 PM EST Project Member

**Labels:** -relnotes\_update\_needed