

39

Information disclosure-Referer leak

Share:



TIMELINE



kkarfalcon submitted a report to [Brave Software](#).

Sep 12th (about 1 year ago)

Assigned to: Brave

Assigned by: Kirtikumar Anandrao Ramchandani

Assigned on: 13/09/2021

Browser information used to test (Up to date):

Code 192 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 Brave      1.29.79 Chromium: 93.0.4577.63 (Official Build) (64-bit)
2 Revision   ff5c0da2ec0adeaed5550e6c7e98417dac77d98a-refs/branch-heads/4577@{#1135}
3 OS        Windows 10 OS Version 2009 (Build 19043.1165)
```

Vulnerability name: Information Disclosure

Vulnerability description: Brave browser has a function of `New Private Window with Tor`.

The browser when used with Tor shouldn't leak the referer.

Steps to reproduce:

1. Visit [exploit](#).
2. Click on `https://www.whatismybrowser.com/`.

Expected behavior: It should have shown a blank `referrer`

Actual behavior: It shows the referrer as: `kirtikumarar.com` which was the host from where we navigated

To know expected behavior, please refer to the below screenshot:

Image F1445735: referrer.PNG 102.75 KiB

[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)



Video POC showing the expected behavior can be found below:

Video F1445736: F-Secure_SAFE.mp4 2.27 MiB


[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)



0:00 / 0:17

Impact


1. This will leak users information
2. In the Tor network, we don't have common URLs as we have in the browsers. They usually are something like `dhxnafkax1xdnackeudxdca.onion`, those can be leaked.

 [diracdeltas](#) Brave Software staff posted a comment.
thanks, we are investigating

Sep 13th (about 1 year ago)

 [diracdeltas](#) Brave Software staff changed the status to Triaged.


Sep 16th (about 1 year ago)

 [kkarfalcon](#) posted a comment.
Respected sir/ma'am,


Sep 16th (about 1 year ago)

Thank you very much quick updates. Can we please add [@HomeSen](#) into the report as a collaborator of this vulnerability? Thanks in advance.

Regards,
Kirtikumar A. R.

 [diracdeltas](#) Brave Software staff posted a comment.
invited

Sep 16th (about 1 year ago)


 [homesen](#) joined this report as a participant.

Sep 16th (about 1 year ago)

 [kkarfalcon](#) posted a comment.

Sep 17th (about 1 year ago)

Thank you very much for the quick update. How can we acknowledge [@homesen](#) as the issue was triaged before he was added? Are we allowed to add another issue of Tor in this case itself?


 [diracdeltas](#) Brave Software staff posted a comment.
i'm not sure if that is possible. you can open a new issue though.

Sep 17th (about 1 year ago)

 [kkarfalcon](#) posted a comment.

Sep 17th (about 1 year ago)

Ok, thank you for swift response, again. Making a report of Tor for a new case with poc.

 [diracdeltas](#) Brave Software staff updated the severity from Medium to High.
we consider this a high privacy issue since it affects Tor

Oct 1st (about 1 year ago)

 [Brave Software](#) rewarded [kkarfalcon](#) with a \$500 bounty.

Oct 1st (about 1 year ago)


I thank you very much for the swift update!

we consider this a high privacy issue since it affects Tor

Reasonable. The idea of leaking `.onion` URLs of [@homesen](#) was a nice one. Due to the reason that I wasn't allowed to add him after completion of my report, he hasn't received an acknowledgment, anyway, we can acknowledge him?

As per rules, we won't disclose the case until the case is patched. Thank you very much for your swift response and a really great co-operation with reporters. It was great working with the Brave team as always. Cheers!

Regards,
Kirtikumar A. R.

 [diracdeltas](#) Brave Software staff posted a comment.

Oct 1st (about 1 year ago)

Sorry I'm not sure how to acknowledge [@homesen](#) on this report. You might need to contact HackerOne support to ask them how to do this.


 [kkarfalcon](#) posted a comment.

Nov 8th (about 1 year ago)

Friendly ping. As we're are planning to write a blog on this case, can you please provide consent?

Note: We will disclose the case if we have proper consent and also after a sufficient number of days- stable build. Once the stable channel is released, we'll wait until all the users receive the patch, and then, when the team is ready to make it public, we'll write about it. Unless we have proper consent, we won't make anything public.

By that time, Happy Diwali. Thanks for your co-operation. :-)

 [diracdeltas](#) Brave Software staff posted a comment.


Nov 8th (about 1 year ago)

[@fmarier](#) is wrapping up the fix now and we're happy to review a blog post in the meantime.

 [kkarfalcon](#) posted a comment.

Nov 8th (about 1 year ago)

Beginning to work on the blogspot today, we'll share it by tomorrow. Thanks for quick update. :)

 [fmarier](#) Brave Software staff posted a comment.

Nov 8th (about 1 year ago)



kkarfalcon posted a comment.

Nov 9th (about 1 year ago)

Hello,

Good morning. That's neat! The remaining all seems to be ok too, there doesn't seem to be any Omibox leakage too (From the available test cases). Once Nightly build with a patch is released, let us know. So, we can add the patch PoC to the blog. Thanks for a quick update, triage, and patch.

Have a nice day!



fmarier Brave Software staff posted a comment.

Nov 18th (about 1 year ago)

My fix has just been merged: <https://github.com/brave/brave-core/pull/10760>

It should be available in the next Nightly build tomorrow so if you'd like to re-test, that would be great.



fmarier Brave Software staff posted a comment.

Nov 18th (about 1 year ago)

next Nightly build tomorrow

That will be going out in approximately 12-16 hours. So if you re-test in 24 hours, you should have the fix.



kkarfalcon posted a comment.

Nov 18th (about 1 year ago)

Hi,

Ok yes. I will re-test and revert back to this report. By that time, can PTAL on the mail I have sent related to blog? Thanks!



kkarfalcon posted a comment.

Nov 19th (about 1 year ago)

Hi,


Neat. The issue has been patched in the:

Code 196 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 Brave      1.34.23 Chromium: 96.0.4664.45 (Official Build) nightly (64-bit)
2 Revision 76e4c1bb2ab4671b8beba3444e61c0f17584b2fc-refs/branch-heads/4664@{#947}
3 OS        Windows 10 Version 21H1 (Build 19043.1348)
```

The stable release is after a week or two? Great work!

 **fmarier** Brave Software staff posted a comment.

Nov 19th (about 1 year ago)

Right now it's available in Brave 1.34, which is scheduled for general release in early January: <https://github.com/brave/brave-browser/wiki/Brave-Release-Schedule#release-channel-dates>

However, I have requested an uplift to 1.33: <https://github.com/brave/brave-core/pull/11186>. If that's approved by the release team, then it will go out to users in early December.

 **kkarfalcon** posted a comment.

Updated Nov 20th (about 1 year ago)

Right now it's available in Brave 1.34, which is scheduled for general release in early **January**

In my current Brave build, it isn't reproducible (before December itself?).


However, I have requested an uplift to **1.33**. If that's approved by the release team, then it will go out to users in early December.

The issue isn't reproducible in 1.32 too. Was it backported? Tested on:

Code 143 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 Brave      1.32.106 Chromium: 96.0.4664.45 (Official Build) (64-bit)
2 Revision 76e4c1bb2ab4671b8beba3444e61c0f17584b2fc-refs/branch-heads/4664@{#947}
```

 **fmarier** Brave Software staff posted a comment.

Nov 20th (about 1 year ago)


No, it wasn't backported. It's only fixed in 1.34.

I just re-tested myself in 1.33 and it's leaking Referer & Origin there. Are you sure you're running the same test as before?

 **kkarfalcon** posted a comment.

Nov 20th (about 1 year ago)

Yes on =<1.33 it is leaking. Sorry was running another referrer test case.

 **fmarier** Brave Software staff posted a comment.

Nov 26th (about 1 year ago)

My fix was uplifted into 1.33 and so it will be part of the December release of Brave.

 **kkarfalcon** posted a comment.

Nov 26th (about 1 year ago)



fmarier

Brave Software staff

posted a comment.

Nov 26th (about 1 year ago)

3 weeks from the date of release we will be making case/blog public

That sounds good. It will give people a good amount of time to upgrade to the latest version.



kkarfalcon

posted a comment.

Nov 27th (12 months ago)

Fine sir. Thank you!



kkarfalcon

requested to disclose this report.

Feb 1st (10 months ago)

As per the discussion, can we disclose the vulnerability report today? It was really great working with the Brave security team especially @diracdeltas (Yan) and @fmarier (Francois). Credits for this vulnerability are also to Patrick Walker (@HomeSen). Cheers! :)



fmarier

Brave Software staff

agreed to disclose this report.

Feb 1st (10 months ago)



This report has been disclosed.

Feb 1st (10 months ago)