Brave Browser permanently timestamps & logs connection times for all v2 domains ~/.config/BraveSoftware/Brave-Browser/tor/dat

Share: **f y** in Y

TIMELINE

kcodes submitted a report to Brave Software. ummary:

Jul 1st (about 1 year ago)

A vulnerability in the Brave Browser v1.28.43 and below allows a local or physical attacker to view the exact timestamps that a user connected to a v2 onion address. A $local\ or\ physical\ attacker\ could\ read\ -/.config/BraveSoftware/Brave-Browser/tor/data/tor.log\ identify\ the\ exact\ moment\ a\ user\ connected\ to\ a\ new\ site,\ easily\ density\ dens$ triangulating the user via a complete log of connection timestamps, which could be easily compared with a server connection log, a compromised Tor end point, or other related Tor attack, affecting the confidentiality & integrity of a user's Tor session.

Products affected:

• operating system, Brave version or Brave website page, etc.

Tor Desktop Browser (All platforms)

Steps To Reproduce:

List the steps needed to reproduce the vulnerability

Visit http://wikitoronionlinks.com/ while using Tor Private Browsing.

Click on an assortment of .onion v2 URLs.

Inspect ~/.config/BraveSoftware/Brave-Browser/tor/data/tor.log

Supporting Material/References:

Code 5 74 KiB 1 Jul 01 08:40:50.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 2 Jul 01 08:40:50.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 3 Jul 01 08:40:51.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 4 Jul 01 08:40:51.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 5 Jul 01 08:40:51.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 6 Jul 01 08:40:52.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 7 Jul 01 08:40:53.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 8 Jul 01 08:40:59.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supr 9 Jul 01 08:40:59.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp 10 Jul 01 08:41:00.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sur 11 Jul 01 08:41:02.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer suc 12 Jul 01 08:41:02.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer suc 13 Jul 01 08:41:02.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sur 14 Jul 01 08:41:07.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sur 15 Jul 01 08:41:07.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sur 16 Jul 01 08:41:09.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer suc 17 Jul 01 08:41:09.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer suc 18 Jul 01 08:41:09.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sur 19 Jul 01 08:41:10.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sur 20 Jul 01 08:41:12.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer sup 21

Impact

Violate the confidentiality & integrity of a user's Tor session.

2 attachments:

F1360378: Screenshot 2021-07-01 08-41-05.png F1360379: Screenshot_2021-07-01_08-50-25.png



Jul 1st (about 1 year ago)

thanks for the report. I would actually suggest opening this as an issue with Tor project since this also affects tor browser.

https://gitlab.torproject.org/tpo/applications/tor-browser/-/issues

as for brave i think we should just reduce LogTimeGranularity. we definitely still want to log messages that are warn or error. maybe tor project should change this warning to a notice and brave should stop logging notices.



Jul 1st (about 1 year ago)

O-diracdeltas Brave Software staff updated the severity from High (7.3) to Low.

Jul 1st (about 1 year ago)

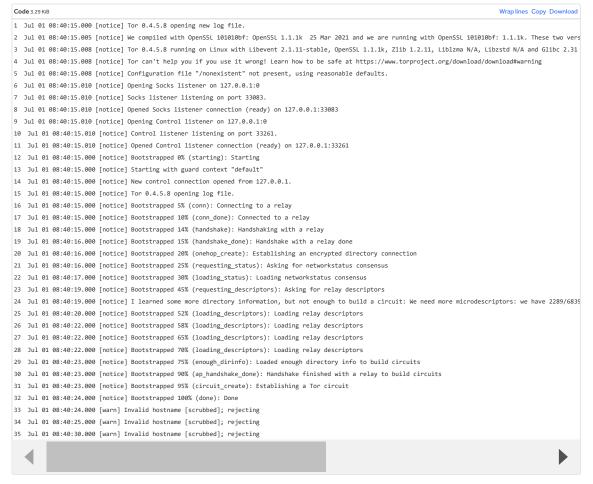
sickcodes posted a comment

Inside of [tor.log], Brave stores the warnings, along with probably a some other info that shouldn't be there,

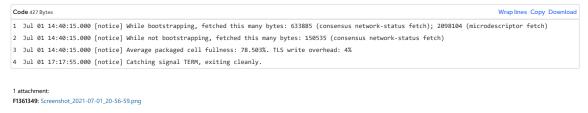
May I suggest disabling Tor logging by default?

Also, for the score, I was basing it off of the last one, which NIST gave a 5.5: https://nvd.nist.gov/vuln/detail/CVE-2020-8276

I think this one is significantly more detailed logging than the first vulnerability, including:



Namely the following:





Jul 1st (about 1 year ago)



Jul 1st (about 1 year ago)



Jul 2nd (about 1 year ago)

 $Removing \ the \ tor \ log \ is \ a \ great \ idea, \ or \ at \ least \ disabling \ it \ by \ default \ would \ be \ nice, \ since \ it's \ quite \ verbose.$

Could we get a CVE issued for this one too once the tor log is removed? I think It would encourage end users to immediately upgrade to latest release once fixed.

Alternatively, could simply:

- disable tor logging by default (switch to opt-in only for debugging)
- rm/delete/shred the log file on exit

 $Although \ Tor \ Project's \ Tor \ doesn't \ log \ to \ disk, it \ still \ logs \ to \ memory, so \ l \ will \ raise \ a \ private \ issue \ to \ the \ Tor \ project \ as \ well.$

Thanks again!

