

19

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

Share:     

TIMELINE



sickcodes submitted a report to Brave Software.

Jul 1st (about 1 year ago)

Summary:

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

```
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 supp
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 08:41:02.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supp
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 supp
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 supp
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 supp
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 supp
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 supp
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 supp
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 supp
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 supp
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 supp
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 supp
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



diracdelatas Brave Software staff posted a comment.

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.



diracdelatas Brave Software staff posted a comment.

Jul 1st (about 1 year ago)

actually we do need notice messages for tor bootstrapping issues



diracdelatas Brave Software staff updated the severity from High (7.3) to Low.

Jul 1st (about 1 year ago)

sickcodes posted a comment.

Jul 1st (about 1 year ago)

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:

Code 3.29 KiB [Wrap lines](#) [Copy](#) [Download](#)

```
1 Jul 01 08:40:15.000 [notice] Tor 0.4.5.8 opening new log file.
2 Jul 01 08:40:15.005 [notice] We compiled with OpenSSL 101010bf: OpenSSL 1.1.1k 25 Mar 2021 and we are running with OpenSSL 101010bf: 1.1.1k. These two vers
3 Jul 01 08:40:15.008 [notice] Tor 0.4.5.8 running on Linux with Libevent 2.1.11-stable, OpenSSL 1.1.1k, Zlib 1.2.11, Liblzma N/A, Libzstd N/A and Glibc 2.31
4 Jul 01 08:40:15.008 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
5 Jul 01 08:40:15.008 [notice] Configuration file "/nonexistent" not present, using reasonable defaults.
6 Jul 01 08:40:15.010 [notice] Opening Socks listener on 127.0.0.1:0
7 Jul 01 08:40:15.010 [notice] Socks listener listening on port 33083.
8 Jul 01 08:40:15.010 [notice] Opened Socks listener connection (ready) on 127.0.0.1:33083
9 Jul 01 08:40:15.010 [notice] Opening Control listener on 127.0.0.1:0
10 Jul 01 08:40:15.010 [notice] Control listener listening on port 33261.
11 Jul 01 08:40:15.010 [notice] Opened Control listener connection (ready) on 127.0.0.1:33261
12 Jul 01 08:40:15.000 [notice] Bootstrapped 0% (starting): Starting
13 Jul 01 08:40:15.000 [notice] Starting with guard context "default"
14 Jul 01 08:40:15.000 [notice] New control connection opened from 127.0.0.1.
15 Jul 01 08:40:15.000 [notice] Tor 0.4.5.8 opening log file.
16 Jul 01 08:40:15.000 [notice] Bootstrapped 5% (conn): Connecting to a relay
17 Jul 01 08:40:15.000 [notice] Bootstrapped 10% (conn_done): Connected to a relay
18 Jul 01 08:40:15.000 [notice] Bootstrapped 14% (handshake): Handshaking with a relay
19 Jul 01 08:40:16.000 [notice] Bootstrapped 15% (handshake_done): Handshake with a relay done
20 Jul 01 08:40:16.000 [notice] Bootstrapped 20% (onehop_create): Establishing an encrypted directory connection
21 Jul 01 08:40:16.000 [notice] Bootstrapped 25% (requesting_status): Asking for networkstatus consensus
22 Jul 01 08:40:17.000 [notice] Bootstrapped 30% (loading_status): Loading networkstatus consensus
23 Jul 01 08:40:19.000 [notice] Bootstrapped 45% (requesting_descriptors): Asking for relay descriptors
24 Jul 01 08:40:19.000 [notice] I learned some more directory information, but not enough to build a circuit: We need more microdescriptors: we have 2289/6835
25 Jul 01 08:40:20.000 [notice] Bootstrapped 52% (loading_descriptors): Loading relay descriptors
26 Jul 01 08:40:22.000 [notice] Bootstrapped 58% (loading_descriptors): Loading relay descriptors
27 Jul 01 08:40:22.000 [notice] Bootstrapped 65% (loading_descriptors): Loading relay descriptors
28 Jul 01 08:40:22.000 [notice] Bootstrapped 70% (loading_descriptors): Loading relay descriptors
29 Jul 01 08:40:23.000 [notice] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits
30 Jul 01 08:40:23.000 [notice] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build circuits
31 Jul 01 08:40:23.000 [notice] Bootstrapped 95% (circuit_create): Establishing a Tor circuit
32 Jul 01 08:40:24.000 [notice] Bootstrapped 100% (done): Done
33 Jul 01 08:40:24.000 [warn] Invalid hostname [scrubbed]; rejecting
34 Jul 01 08:40:25.000 [warn] Invalid hostname [scrubbed]; rejecting
35 Jul 01 08:40:30.000 [warn] Invalid hostname [scrubbed]; rejecting
```

Namely the following:

Code 427 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1 Jul 01 14:40:15.000 [notice] While bootstrapping, fetched this many bytes: 633885 (consensus network-status fetch); 2098104 (microdescriptor fetch)
2 Jul 01 14:40:15.000 [notice] While not bootstrapping, fetched this many bytes: 150535 (consensus network-status fetch)
3 Jul 01 14:40:15.000 [notice] Average packaged cell fullness: 78.503%. TLS write overhead: 4%
4 Jul 01 17:17:55.000 [notice] Catching signal TERM, exiting cleanly.
```

1 attachment:

F1361349: Screenshot_2021-07-01_20-56-59.png

 **dirac deltas** Brave Software staff updated the severity from Low to Medium. Jul 1st (about 1 year ago)

 **dirac deltas** Brave Software staff posted a comment. Jul 1st (about 1 year ago)

thanks we are looking into getting rid of the log file

 **Sickcodes** posted a comment. Jul 2nd (about 1 year ago)

Thank you very much for the score update 😊

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 I will raise a private issue to the Tor project as well.


Thanks again!


-  Brave Software rewarded [sickcodes](#) with a \$400 bounty.


Jul 7th (about 1 year ago)
-  [sickcodes](#) posted a comment.
Thank you very much! <3


Jul 7th (about 1 year ago)
- FYI: Tor project closed the report regarding v2 connection timestamps as informative and will not be removing the timestamps.
-  sickcodes requested to disclose this report.

Jul 16th (about 1 year ago)
-  [diracdeltas](#) Brave Software staff posted a comment.
CVE-2021-22929 has been requested. I'll disclose this report soon after 1.28.x reaches stable.

Jul 16th (about 1 year ago)
-  sickcodes posted a comment.
Thanks [@diracdeltas](#), I saw a few releases and assumed it was already mainline. Take your time :)

Jul 16th (about 1 year ago)
-  sickcodes requested to disclose this report.

Aug 16th (about 1 year ago)
-  This report has been disclosed.

Aug 16th (about 1 year ago)
-  sickcodes posted a comment.
Thank you very much [@diracdeltas](#)!

Aug 21st (about 1 year ago)
- The CVE ID is still listed as None, and I did reach out to MITRE but as H1 is the CNA, I wasn't able to add references.


Would you be able to add these to the references on the advisory for CVE-2021-22929?


<https://github.com/brave/brave-core/pull/9346>

<https://hackerone.com/reports/1249056>

<https://www.privacyaffairs.com/cve-2021-22929-brave-tor-vulnerability/>

<https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-109.md>

<https://sick.codes/sick-2021-109>
-  [diracdeltas](#) Brave Software staff posted a comment.
I cannot edit it either and it says "pending hackerone approval". [@jgarza](#) are you able to edit the CVE request?

Aug 22nd (about 1 year ago)
-  sickcodes posted a comment.
I emailed support and they published the CVE, thank you [@diracdeltas](#)!

Sep 1st (about 1 year ago)