6 Brave Browser potentially logs the last time a Tor window was used

Share:

TIMELINE

sickcodes submitted a report to Brave Software. Nov 2nd (2 ye

Summary:

A vulnerability in the Brave Browser allows an attacker to view the last time a Tor session was used in incognito mode. A local, on-disk attacker could read the Brav Browser's "Local State" json file and identify the last time a Tor session was used, affecting the confidentiality of a user's Tor session.

For example, the "Local State" file of a user who has recently used a Tor session would list a key value pair with a timestamp as accurate as "13248493693576042" allows an attacker to fingerprint, or prove beyond reasonable doubt, that a user was using Tor at that very specific moment in time.

Products affected:

Brave 1.18.27 and below

Steps To Reproduce:

Start a Tor session in Brave Browser

Supporting Material/References:

As discussed with security@ team in email chain titled:

Re: [Security] CVE Request 981386 - Brave Browser (All) - Exposure of
Sensitive Information to an Unauthorized Actor While Using Tor Feature

And fixed in PR 7010:
https://github.com/brave/brave-core/pull/7010

- List any additional material (e.g. screenshots, logs, etc.)

Impact

Violate the confidentiality of a user's Tor session.

diracdeltas Brave Software staff changed the status to **Triaged**. Nov 2nd (2 ye

diracdeltas Brave Software staff posted a comment. Updated Nov 2nd (2 ye

my response from the email thread:

I think this is a sec-low issue given that someone who has access to the local disk cannot tell if the timestamp corresponds to a Tor session (rather than a regular incognito session). Also, the value that actually gets sent to the Brave metrics server is bucketed into the following values (so the timestamp isn't a fingerprinting vector):

Code 125 Bytes Wrap lines Copy Dow

```
1 Used in last 24h
2 Used in last week but not 24h
3 Used in last 28 days but not week
4 Ever used but not in last 28 days
5 Never used
```

Brave Software rewarded sickcodes with a **$100** bounty. Nov 2nd (2 ye

sickcodes posted a comment. Nov 2nd (2 ye

Thank you very very much! Feel free to adjust the title/description as appropriate.

diracdeltas Brave Software staff closed the report and changed the status to **Resolved**. Nov 4th (2 ye

This has been fixed in nightly. CVE request submitted.

diracdeltas Brave Software staff requested to disclose this report. Nov 4th (2 ye

Report needs to be public before CVE request is approved.

Nov 4th (2 years ago)
diracdeltas Brave Software staff
changed the report title from **Brave Browser Tor Session Logging via Timestamp in Local State File Stored On-Disk** to **Brave Browser potentially logs the last time a Tor window was used**.

sickcodes agreed to disclose this report. Nov 4th (2 ye

This report has been disclosed. Nov 4th (2 ye

sickcodes posted a comment. Nov 4th (2 ye

Code 75 Bytes Wrap lines Copy Dow

```
jq '.core_p3a_metrics' < ~/.config/BraveSoftware/Brave-Browser/Local\ State
```

Returns

Code 73 Bytes Wrap lines Copy Dow

```
{
  "incognito_used_timestamp": "13248495136836403",
  "tor_used": true
}
```

Feel free to upgrade the severity of this report if this changes perspective.

1 attachment:
F1065667: Screenshot_2020-11-05_03-51-42.png

tracdeltas Brave Software staff posted a comment. Nov 4th (2 ye

@sickcodes tor_used is just whether tor was ever used (since you downloaded brave), not necessarily whether the last incognito session was a tor session

sickcodes posted a comment. Nov 4th (2 ye

Thanks for pointing that out; I confirm that is true:

Open incognito with Tor:

Code 73 Bytes Wrap lines Copy Dow

```
{
  "incognito_used_timestamp": "13249022386728896",
  "tor_used": true
}
```

Open incognito without Tor:

Code 73 Bytes Wrap lines Copy Dow

```
{
  "incognito_used_timestamp": "13249022400646476",
  "tor_used": true
}
```

On a related note, is there any particular reason why logging (in general) requires nanosecond accuracy?

sickcodes posted a comment. Nov 4th (2 ye

Published on https://sick.codes/sick-2020-013/
Published on https://github.com/sickcodes/security/blob/master/advisories/SICK-2020-013.md

sickcodes posted a comment. Nov 24th (2 ye

Hi all, NIST scored this one a medium 5.5 https://nvd.nist.gov/vuln/detail/CVE-2020-8276

Not sure if you wanted to update the score of the report above, but it would cool on my HackerOne profile if this was a medium as I know you have different intern scores. Otherwise, happy to leave as-is!