sickcodes [CVE-2021-39246] 6.1 CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N ✓ History

1 contributor

110 lines (63 sloc) | 4.97 KB

Title

CVE-2021-39246 - Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack excessive verbose logging - Windows, macOS, Linux

CVE ID

CVE-2021-39246

CVSS Score

6.1

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Internal ID

SICK-2021-111

Vendor

Tor

Product

Tor Browser on Windows, macOS, Linux

Product Versions

10.5.6 and 11.x through 11.0a4

Vulnerability Details

Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network). This occurs by default, with or without verbose.

Vendor Response

Open pull request in relation to timestamp logging as v2 will be deprecated soon:

https://gitlab.torproject.org/tpo/core/tor/-/merge_requests/434.

Proof of Concept

`Tor Browser` latest `10.5.6` is affected.

`Tor Browser` alpha `11.0a4` is affected.

This is because `Tor 0.4.6` introduced a warning every time a client connects to a v2 domain.

See: https://gitlab.torproject.org/tpo/core/tor/-/commit/5e836eb80c31b97f87b152351b6a7a932aeffaed

Also see "Log warning when connecting to soon-to-be-deprecated v2 onions."

https://gitlab.torproject.org/tpo/core/tor/-/commit/80c404c4b79f3bcba3fc4585d4c62a62a04f3ed9

```
cd /tmp

wget https://www.torproject.org/dist/torbrowser/10.5.6/tor-browser-linux64-10.5.6_en-US.tar.xz

tar -xzvf tor-browser-linux64-10.5.6_en-US.tar.xz

cd /tmp/tor-browser_en-US/

./start-tor-browser.desktop --verbose

# Launching './Browser/start-tor-browser --detach --verbose'...
```

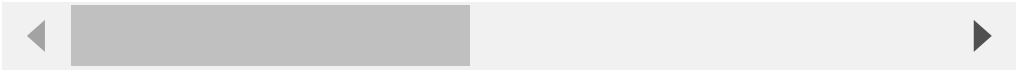
Visit any v2 onion site, connection timestamps are logged at the exact moment the server responds.

```
Sep 24 16:28:52.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons,

Sep 24 16:28:52.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons,

Sep 24 16:28:52.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons,

Sep 24 16:29:02.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons,
```



Disclosure Timeline

- **2021-07-02** - Researcher discovers vulnerability on bounty platform
- **2021-07-07** - Report closed as informative
- **2021-08-17** - Researcher requests CVE
- **2021-08-17** - Vendor re-notified via sec mailing list, and on bounty platform chat.
- **2021-09-10** - No response: researcher opens Pull Request to remove timestamps.
- **2021-09-24** - CVE published

Links

https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-111.md

https://sick.codes/sick-2021-111

https://www.privacyaffairs.com/cve-2021-39246-tor-vulnerability/

https://gitlab.torproject.org/tpo/core/tor/-/commit/80c404c4b79f3bcba3fc4585d4c62a62a04f3ed9

https://gitlab.torproject.org/tpo/core/tor/-/merge_requests/434

https://hackerone.com/reports/1250273

Researchers

- *Sick Codes* https://github.com/sickcodes || https://twitter.com/sickcodes
- *Miklos Zoltan* https://twitter.com/mzb4455 || https://www.privacyaffairs.com/authors/miklos/

CVE Links

https://sick.codes/sick-2021-111

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39246

https://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-39246