

SICK.CODES

HOME RELEASES SUBMIT VULN PRESS ABOUT PGP CONTACT ▾ TUTORIALS ▾ SUPPORTERS PROJECTS



Home > Security

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

by Sick Codes – September 24, 2021 - Updated on October 4, 2021 in Security 2

2 changed files ▾

src/core/or/connection_edge.c



```

2530 +
2531 + /* We don't support v2 onions anymore. Log a warning and bail. */
2532 + if (addresstype == ONION_V2_HOSTNAME) {
2533 +     log_warn(LD_PROTOCOL, "Tried to connect to a v2 onion address, but this "
2534 +         "version of Tor no longer supports them. Please encourage the "
2535 +         "site operator to upgrade. For more information see "
2536 +         "https://blog.torproject.org/v2-deprecation-timeline.");
2537 +     control_event_client_status(LOG_WARN, "SOCKS_BAD_HOSTNAME HOSTNAME=%s",
2538 +         escaped(socks->address));
2539 +     connection_mark_unattached_ap(conn, END_STREAM_REASON_TORPROTOCOL);
2540 +     return -1;
2541 + }
2542 +
2543 tor_assert(addresstype == ONION_V3_HOSTNAME);

```

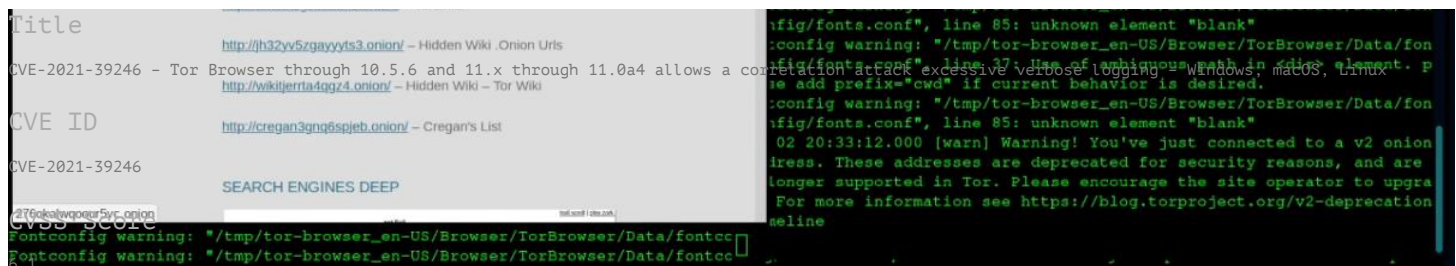
CVE 2021 39246 Tor Browser through 10.5.6 and 11.x through 11.0a4

The screenshot shows a Tor Browser window with several tabs open. The active tab is 'wikitoronionlinks.com', which displays a list of onion links categorized by type (e.g., Wiki Links, LINK DIR ONION, LINKS TOR 2018, Links Dir Tor onion, Wiki site Tor, Dark ONION Dir - Best urls, Uncensored Hidden Wiki, Dir Link, HD Wiki, List of random links, Onion Wiki - 650+ working 05.2017 deep web links, TorLinks). The terminal window on the right shows the following output:

```

user@hostname: /tmp/tor-browser_en-US - Terminal
Edit View Terminal Tabs Help
For more information see https://blog.torproject.org/v2-deprecation-timeline
:config warning: "/tmp/tor-browser_en-US/Browser/TorBrowser/Data/fon
:fig/fonts.conf", line 37: Use of ambiguous path in <dir> element. p
:se add prefix="cwd" if current behavior is desired.
:config warning: "/tmp/tor-browser_en-US/Browser/TorBrowser/Data/fon
:fig/fonts.conf", line 85: unknown element "blank"
:config warning: "/tmp/tor-browser_en-US/Browser/TorBrowser/Data/fon
:fig/fonts.conf", line 37: Use of ambiguous path in <dir> element. p
:se add prefix="cwd" if current behavior is desired.
:config warning: "/tmp/tor-browser_en-US/Browser/TorBrowser/Data/fon
:fig/fonts.conf", line 85: unknown element "blank"
02 20:33:11.000 [warn] Warning! You've just connected to a v2 onion
dress. These addresses are deprecated for security reasons, and are
longer supported in Tor. Please encourage the site operator to upgra
For more information see https://blog.torproject.org/v2-deprecation
seline
02 20:33:12.000 [warn] Warning! You've just connected to a v2 onion
dress. These addresses are deprecated for security reasons, and are
longer supported in Tor. Please encourage the site operator to upgra
For more information see https://blog.torproject.org/v2-deprecation
seline
:config warning: "/tmp/tor-browser_en-US/Browser/TorBrowser/Data/fon
:fig/fonts.conf", line 37: Use of ambiguous path in <dir> element. p
:se add prefix="cwd" if current behavior is desired.
:config warning: "/tmp/tor-browser_en-US/Browser/TorBrowser/Data/fon

```



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 -xvzf 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, and are no longer supported in Tor. Please encourage the site operator to upgrade. For more information see <https://blog.torproject.org/v2-deprecation-timeline>

Sep 24 16:28:52.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supported in Tor. Please encourage the site operator to upgrade. For more information see <https://blog.torproject.org/v2-deprecation-timeline>

Sep 24 16:28:52.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supported in Tor. Please encourage the site operator to upgrade. For more information see <https://blog.torproject.org/v2-deprecation-timeline>

Sep 24 16:29:02.000 [warn] Warning! You've just connected to a v2 onion address. These addresses are deprecated for security reasons, and are no longer supported in Tor. Please encourage the site operator to upgrade. For more information see <https://blog.torproject.org/v2-deprecation-timeline>

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>

Comments 2

Pingback: Vulnerability Summary for the Week of September 27, 2021 | Smart Cyber Security

Pingback: Vulnerabilidad en () - CVE-2021-39246 - Información y Soluciones

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

POST COMMENT



@sickcodes



@sickcodes



@sickcodes



Discord Server



sickcodes.slack.com



t.me/sickcodeschat



./contact_form