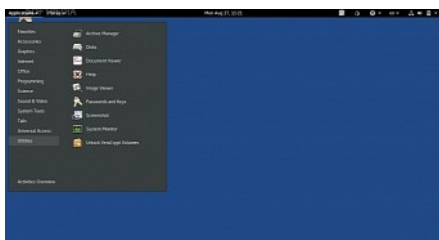


# Tails 3.14 Anonymous Linux OS Adds Mitigations for the Intel MDS Vulnerabilities

By *Rianne Schestowitz*

Created 23/05/2019 - 7:58pm

Submitted by Rianne Schestowitz on Thursday 23rd of May 2019 07:58:58 PM Filed under [Security](#) [1]



Tails 3.14 is here two months after the release of Tails 3.13 mainly to address the recently discovered MDS (Microarchitectural Data Sampling) security vulnerabilities in Intel microprocessors. To fully mitigate these flaws and protect you against Fallout, RIDL, and ZombieLoad attacks, the SMT function must be disabled.

Furthermore, Tails 3.14 ships with long-term supported Linux 4.19.37 kernel and the all the latest firmware packages to provide you with up-to-date hardware support and compatibility with newer graphics and Wi-Fi devices, as well as other components, and utilizes the recently released TOR Browser 8.5 anonymous web browser.

[2]

[Security](#)

---

**Source URL:** <http://www.tuxmachines.org/node/124184>

## Links:

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] <https://news.softpedia.com/news/tails-3-14-anonymous-linux-os-adds-mitigations-for-the-intel-mds-vulnerabilities-526147.shtml>