# Security-Oriented Container Linux Gets Patched Against Latest Intel CPU Flaws

By *Roy Schestowitz*
Created *21/11/2019 - 1:21pm*
Submitted by Roy Schestowitz on Thursday 21st of November 2019 01:21:27 PM Filed under GNU [1] Linux [2] Security [3]


The security-oriented Container Linux by CoreOS GNU/Linux distribution has been updated this week with all the necessary patches to mitigate the latest Intel CPU microarchitecture vulnerabilities.

CoreOS Container Linux 2247.7.0 is here as the latest stable version of the security-oriented, minimal operating system for running containerized workloads securely and at scale, which was acquired by Red Hat last year and will soon become Fedora CoreOS. This release includes fixes for the CVE-2019-11135 and CVE-2018-12207 security vulnerabilities affecting Intel CPUs.

According to the release notes, CoreOS Container Linux 2247.7.0 fixes Intel CPU disclosure of memory to user process, but the complete mitigation requires manually disabling TSX or SMT on affected processors. Additionally, is also fixes Intel CPU denial of service by a malicious guest VM, and a CFS scheduler bug throttling highly-threaded I/O-bound applications.

[4]

GNU Linux Security

---

**Source URL:** http://www.tuxmachines.org/node/130769

**Links:**
[1] http://www.tuxmachines.org/taxonomy/term/144
[2] http://www.tuxmachines.org/taxonomy/term/63
[3] http://www.tuxmachines.org/taxonomy/term/59
[4] https://news.softpedia.com/news/security-oriented-container-linux-gets-patched-against-latest-intel-cpu-flaws-528253.shtml