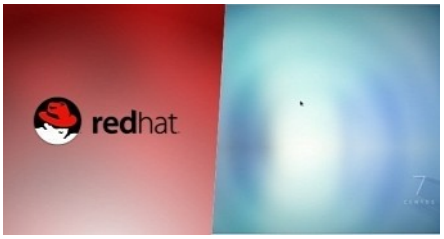
# Red Hat Enterprise Linux and CentOS Now Patched Against Latest Intel CPU Flaws

By *Rianne Schestowitz*
Created *16/11/2019 - 8:22pm*
Submitted by Rianne Schestowitz on Saturday 16th of November 2019 08:22:54 PM Filed under Linux [1] Red Hat [2] Security [3]




After responding to the latest security vulnerabilities affecting Intel CPU microarchitectures, Red Hat has released new Linux kernel security updates for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 operating systems to address the well-known ZombieLoad v2 flaw and other issues. The CentOS community also ported the updates for their CentOS Linux 6 and CentOS Linux 7 systems.

The security vulnerabilities patched in this new Linux kernel security update are Machine Check Error on Page Size Change (IFU) (CVE-2018-12207), TSX Transaction Asynchronous Abort (TAA) (CVE-2019-11135), Intel GPU Denial Of Service while accessing MMIO in lower power state (CVE-2019-0154), and Intel GPU blitter manipulation that allows for arbitrary kernel memory write (CVE-2019-0155).

[4]

Linux Red Hat Security

**Links:**
[1] http://www.tuxmachines.org/taxonomy/term/63
[2] http://www.tuxmachines.org/taxonomy/term/142
[3] http://www.tuxmachines.org/taxonomy/term/59
[4] https://news.softpedia.com/news/red-hat-enterprise-linux-and-centos-now-patched-against-latest-intel-cpu-flaws-528177.shtml