AMD Defects, Linux Affected Also

By *Roy Schestowitz*
Created *11/07/2019 - 11:40am*
Submitted by Roy Schestowitz on Thursday 11th of July 2019 11:40:20 AM Filed under Linux [1] Hardware [2] Security [3]

- **AMD's SEV tech that protects cloud VMs from rogue servers may as well stand for... Still Extremely Vulnerable [4]**

  Five boffins from four US universities have explored AMD's Secure Encrypted Virtualization (SEV) technology ? and found its defenses can be, in certain circumstances, bypassed with a bit of effort.

  In a paper [PDF] presented Tuesday at the ACM Asia Conference on Computer and Communications Security in Auckland, New Zealand, computer scientists Jan Werner (UNC Chapel Hill), Joshua Mason (University of Illinois), Manos Antonakakis (Georgia Tech), Michalis Polychronakis (Stony Brook University), and Fabian Monrose (UNC Chapel Hill) detail two novel attacks that can undo the privacy of protected processor enclaves.

  The paper, "The SEVerESt Of Them All: Inference Attacks Against Secure Virtual Enclaves," describes techniques that can be exploited by rogue cloud server administrators, or hypervisors hijacked by hackers, to figure out what applications are running within an SEV-protected guest virtual machine, even when its RAM is encrypted, and also extract or even inject data within those VMs.

-

AMD Ryzen 3000 is experiencing problems with some Linux distributions [5]

Ryzen 3000 seems to have boot problems with the most modern Linux distributions. The problem affects all operating systems using a 2019 Linux distribution with Linux 5.0/5.1/5.2 kernels.

This problem is now known to be related to the RdRand command. Remember that the previous Ryzen processors were also not friendly when they used the RNG hardware command, which caused problems on the platform. However, now with Zen2, this is even worse supported, and AMD has not yet officially detected the problem.

- **AMD Posts New CPUFreq Driver For CPPC Support With Zen 2 CPUs [6]**

AMD Zen 2 CPUs support ACPI's Collaborative Processor Performance Control (CPPC) for tuning the system to energy and/or performance requirements. AMD has now published a new CPUfreq driver for handling their CPPC implementation and the new controls found with their new processors.

The AMD CPPC support with Zen 2 desktop/server/mobile CPUs can be optionally enabled and allows setting min/maximum performance along with desired performance and other knobs for tuning via sysfs.

Linux Hardware Security

Source URL: http://www.tuxmachines.org/node/125773

Links:
[1] http://www.tuxmachines.org/taxonomy/term/63
[2] http://www.tuxmachines.org/taxonomy/term/39
[3] http://www.tuxmachines.org/taxonomy/term/59
[4] https://www.theregister.co.uk/2019/07/10/amd_secure_enclave_vulnerability/
[5] https://optocrypto.com/amd-ryzen-3000-is-experiencing-problems-with-some-linux-distributions/
[6] https://www.phoronix.com/scan.php?page=news_item&px=AMD-New-CPUFreq-CPPC