Published on *Tux Machines* (http://www.tuxmachines.org)

Home > content > Security Leftovers

Security Leftovers

By *Roy Schestowitz*
Created *22/05/2019 - 7:16pm*
Submitted by Roy Schestowitz on Wednesday 22nd of May 2019 07:16:47 PM Filed under Security [1]

- **Security updates for Wednesday [2]**

- **Illumos-Powered OmniOS Gets Updated Against MDS / ZombieLoad Vulnerabilities [3]**

  > While it was just earlier this month that the OpenSolaris/Illumos-based OmniOS saw a big LTS release, it's already been succeeded by a new release given the recent Intel MDS / Zombieload CPU vulnerabilities coming to light.
  >
  > There are new spins of OmniOS for all supported releases. These new OmniOS Community Edition releases mitigate against the Multiarchitectural Data Sampling (MDS) vulnerabilities and also bundle in the updated Intel CPU microcode.

- **Hackers Hack A Forum For Hacked Accounts: Here?s How [4]**

  > A group of hackers failed to deploy security mechanisms to secure the storage where they store hacked accounts and another hacker group hacked it.
  >
  > The story is indeed funny and real. Infamous forum named OGUSERS which is popular amongst hackers for obtaining ?OG? Instagram, Twitter usernames, hacked accounts of Domino?s Pizza, Steam, PlayStation Network, and other online accounts was hacked by a hacker group and its data was published in another hacker forum.

- **Security Announcement: Disabling SMT by default on affected Intel processors [5]**

This is an important announcement with an upcoming change in the next Core Update of IPFire.

Because of the recent vulnerabilities in Intel processors, the IPFire team has decided, that - to keep systems as secure as possible - Simultaneous Multi-Processing (SMT) is automatically disabled if the processor is vulnerable to one of the attacks.

SMT is also called Intel(R) Hyper-Threading Technology and simulates more virtual cores than the system has. This allows to perform faster processing when applications benefit from it. Unfortunately with networking, we benefit from that. Therefore the effect of disabling SMT will be a very signifiant performance impact of around 30% or more. Applications that will be affected in IPFire are the firewall throughput itself as well as other CPU and memory-bound tasks like the web proxy and the Intrusion Prevention System. On systems that are not vulnerable for this attack, SMT is being left enabled. If you still want to disable it, please do so in the BIOS of your firewall.

Security

Source URL: http://www.tuxmachines.org/node/124152

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/789132/rss
[3] https://www.phoronix.com/scan.php?page=news_item&px=OmniOS-MDS-Mitigated
[4] https://fossbytes.com/hackers-hack-forum-hacked-accounts/
[5] https://blog.ipfire.org/post/security-announcement-disabling-smt-by-default-on-affected-intel-processors