Spectre svuda, Spectre NG oko nas!

Nedavno otkriveni (i potom loše krpani) Spectre i Meltdown propusti u mikrokodu Intelovih procesora, ne previše iznenađujuće, nisu bili i jedini. Novi skup propusta, njih točno osam komada, otkriveni su u Intelovim procesorima. Četiri od njih Intel je označio kao vrlo ozbiljne, a kako prenosi njemački časopis c't (https://www.heise.de/ct/artikel/Exclusive-Spectre-NG-Multiple-new-Intel-CPU-flaws-revealed-several-serious-4040648.html [1]), jedan od napada omoućuje napadaču da iz instance virtualnog poslužitelja napadne računalo na kojem je pokrenut virtualni poslužitelj, ili pak druge virtualne poslužitelje koji se nalaze na istom računalu.

Ovaj scenario je posebice opasan jer u opasnost stavlja ne samo virtualni poslužitelj nekog korisnika, već i ostale virtualne poslužitelje na tom računalu, što bi u teoriji moglo ugroziti i one poslužitelje čiji administratori vrijedno i stručno rade svoj posao, i svoje sustave drže u skladu sa visokim standardima zaštite podataka.

Novi propusti su otkriveni na Intel platformi, no čini se da je dio procesora ARM arhitekture također zahvaćen ovim propustima, a ispitivanje AMD procesora u trenutku pisanja ovog teksta još uvijek traje.

Zakrpa koja je trebala biti izdana danas odgođena (https://www.heise.de/security/meldung/Spectre-NG-Intel-verschiebt-die-ersten-Patches-koordinierte-Veroeffentlichung-aufgeschoben-4043790.html [2]) je za dva tjedna, kako navodi Intel. Praktično, to znači da ćemo vjerojatno zakrpe vidjeti do kraja ovog ili sljedećeg mjeseca, iako nas iskustvo (http://bgr.com/2018/01/22/intel-spectre-patch-performance-bugs-reboot/ [3]) sa prethodnom generacijom zakrpa uči da budemo na oprezu.

Potencijalno traumatičniji problem je što ovi propusti pokazuju kako su proizvođači hardvera, očekivano fokusirani na postizanje što boljih performansi, manje pažnje posvetili sigurnosti svojih inovacija. Ako se nastave otkrivati slični propusti prediktivnog grananja, u budućnosti bismo mogli očekivati izlazak radikalno redizajnirane serije procesora, uz potencijalne probleme sa kompatibilnošću sa starim hardverom ili softverom.

Dodamo li na hardversku priču i onu softversku, uzmemo li u obzir da je Microsoft izdao zakrpu za (staru generaciju) Spectre i Meltdown samo za Windows 10 (a i to nakon par loših pokušaja za koje je dobrim dijelom kriv Intel (https://www.zdnet.com/article/spectre-reboot-problems-now-intel-replaces-its-buggy-fix-for-skylake-pcs/ [4]), a za Windows 7 i 8 ne, konačnu cijenu nepažnje pri dizajniranju procesora platit će krajnji korisnik, dok bi u ovom distopičnom scenariju proizvođači hardvera i softvera na kraju dana mogli i lijepo profitirati.

.

uto, 2018-05-08 14:00 - Radoslav Dejanović**Vijesti:** Sigurnost [5]
Vote: 4

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Vaša ocjena: Nema Average: 4 (1 vote)

story_tag: meltdown [6]
spectre [7]

Source URL: https://sysportal.carnet.hr/node/1805

Links
[1] https://www.heise.de/ct/artikel/Exclusive-Spectre-NG-Multiple-new-Intel-CPU-flaws-revealed-several-serious-4040648.html
[2] https://www.heise.de/security/meldung/Spectre-NG-Intel-verschiebt-die-ersten-Patches-koordinierte-Veroeffentlichung-aufgeschoben-4043790.html
[3] http://bgr.com/2018/01/22/intel-spectre-patch-performance-bugs-reboot/
[4] https://www.zdnet.com/article/spectre-reboot-problems-now-intel-replaces-its-buggy-fix-for-skylake-pcs/
[5] https://sysportal.carnet.hr/taxonomy/term/13
[6] https://sysportal.carnet.hr/taxonomy/term/202
[7] https://sysportal.carnet.hr/taxonomy/term/203

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr