Operacija uspjela, pacijent umro - Meltdown i Spectre!

Intel did it again. Samo što je prošli put (https://en.wikipedia.org/wiki/Pentium_F00F_bug [1]) šteta bila lokalizirana – blokiralo bi se računalo, ali bi korisnički podaci ostali zaštićeni. Ovog puta, iako se još službeno ne zna o čemu je točno riječ, frenetičan rad na izradi sigurnosnih zakrpa za sva tri popularna operacijska sustava (Linux, Mac, Windows) daje naslutiti kako su govorkanja istinita, ili barem blizu istine: hardverski problem u Intelovim procesorima, koji postoji već jedno desetljeće, omogućuje programima u korisničkom prostoru pristup cjelokupnoj memoriji prostora kernela.

Razbijeno na jednostavnije pojmove, podsjetimo se kako je jedna od ključnih značajki modernih operacijskih sustava izolacija procesa, i to ne samo jednog procesa od drugog, već i samog kernela operacijskog sustava od prostora koji je dan na raspolaganje korisničkim programima.

Intelovi procesori, nažalost, čini se imaju kobnu hardversku pogrešku u prediktivnom algoritmu zbog koje korisnički procesi mogu pristupiti informacijama koje se nalaze u prostoru kernela, što je iznimno opasan sigurnosni propust. Preciznije detalje o problemu donosi ArsTechnica (https://arstechnica.com/gadgets/2018/01/whats-behind-the-intel-design-flaw-forcing-numerous-patches/ [2]).

Nažalost, najveći problem ove priče je činjenica da je pogreška u samom hardveru procesora i nije ju moguće promjeniti nadogradnjom mikrokoda ili na bilo koji drugi način osim bacanjem procesora u smeće i kupnjom novog procesora – AMD procesori, primjerice, ne pate od ovog problema.

Kako je bacanje procesora u smeće skupo, nepraktično i ekološki štetno, proizvođači operacijskih sustava prionili su na zaobilaženje ovog problema na relativno jednostavan, ali skup način: potpunim razdvajanjem korisničkih od kernelovih tablica, praktički isključivanjem hardverski ubrzanog rješenja na samom čipu.

Posljedica toga je, očekivano, pad performansi računala. Kako je za svaki syscall i svaki prekid sad potrebno pozivati softversku rutinu koja u tablici kernela sadrži tek minimalnu količinu informacija nužnu za ispravan rad procesora, to znači da se svaki put kad procesor krene izvršavati korisnički program, podaci za kernelovu tablicu moraju iznova napuniti. To stalno punjenje i pražnjenje tablice ima značajne posljedice po performase računala: prema procjenama, usporavanje rada računala kreće se od 2-3%, pa sve do 60%, ovisno o vrsti posla koje računalo obavlja. Praktična mjerenja performansi pokazala su da usporenje uglavnom nije drastično, ali u nekim slučajevima je osjetno: primjerice, PostgreSQL je izvjestio (https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe@alap3.anarazel.de [3]) o mogućem smanjenju performansi poslužitelja baza podataka od 17-23%.

Koliko će se računala usporiti nakon primjene sigurnosne zakrpe ovisi, reklo bi se, o količini sistemskih poziva, pri čemu su I/O pozivi najviše pogođeni. Praktično, to znači da bi uredska i kućna računala trebala biti gotovo beznačajno pogođena, ali poslužitelji sa mnoštvom I/O operacija mogli bi pokazati značajna usporenja u svom radu.

Intel (https://www.marketwatch.com/investing/stock/intc [4]) je zanijekao (http://www.tomshardware.com/news/intel-cpu-bug-amd-performance,36213.html [5]) problem, ali ako za nekoliko dana primjetite da se vaši poslužitelji nekako lijeno ponašaju – znat ćete zbog čega.

Ovakva je situacija nedopustiva, ali nažalost ne možemo učiniti baš ništa osim konkretne zamjene hardvera; ostaviti sustave nezakrpane bilo bi krajnje neodgovorno, a zakrpa bi mogla “postarati” računalo za cijelu jednu generaciju. Mogli bismo to nazvati Pirovom pobjedom, kad bismo to uopće mogli smatrati pobjedom.

sri, 2018-01-03 23:31 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [6]
Kategorije: Hardware [7]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: intel [8]
cpu [9]
procesor [10]
bug [11]
microcode [12]
meltdown [13]
spectre [14]

Source URL: https://sysportal.carnet.hr/node/1784

Links
[1] https://en.wikipedia.org/wiki/Pentium_F00F_bug
[2] https://arstechnica.com/gadgets/2018/01/whats-behind-the-intel-design-flaw-forcing-numerous-patches/
[3] https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe@alap3.anarazel.de
[4] https://www.marketwatch.com/investing/stock/intc
[5] http://www.tomshardware.com/news/intel-cpu-bug-amd-performance,36213.html
[6] https://sysportal.carnet.hr/taxonomy/term/14
[7] https://sysportal.carnet.hr/taxonomy/term/24
[8] https://sysportal.carnet.hr/taxonomy/term/196
[9] https://sysportal.carnet.hr/taxonomy/term/197
[10] https://sysportal.carnet.hr/taxonomy/term/198
[11] https://sysportal.carnet.hr/taxonomy/term/199
[12] https://sysportal.carnet.hr/taxonomy/term/200
[13] https://sysportal.carnet.hr/taxonomy/term/202
[14] https://sysportal.carnet.hr/taxonomy/term/203