Procesory Intel mají vážnou hardwarovou chybu, záplata výrazně snižuje výkon

AMD stále tvrdí, že její CPU nejsou postižena (tedy přesněji řečeno, že nejde ani o zásadní, ani o obecný problém, viz vyjádření společnosti). Linus Torvalds mezitím do jádra začlenil patch, který vypíná ochranu proti této chybě, tedy Page Table Isolation, pro CPU AMD. Google však naopak tvrdí, že postižena jsou i CPU ARM a AMD, nicméně blíže nic neupřesňuje (může jít tedy jen o určité architektury). Na webu Meltdown and Spectre se hovoří o tom, že Meltdown postihuje prakticky všechna CPU od roku 1995 (kromě Intel Itanium a Atomů z doby před 2013). U Spectre je již ověřeno, že postihuje i CPU ARM a AMD.

Bližší detailní informace shrnují dokumenty odkazované v dolní části webu Meltdown and Spectre Google uvádí svá zjištění na webu týmu Zero, resp. svém bezpečnostním blogu.

Úvodem nutno podotknout, že toto není další článek o Intel Management Engine. Jde o zcela jiný problém, pro který je v jádru 4.15 k dispozici sada opravných patchů, které byly/jsou/budou backportovány i do řad 4.14 (aktuální stabilní) a 4.9 (aktuální LTS). Podobnou věc implementují i Windows 10, v Microsoftu se na tom už několik týdnů pracuje.

Špatná implementace u Intelu

Procesory Intel totiž obsahují chybu implementace TLB (Translation Lookaside Buffer, součást CPU s nemalým dopadem na výkon), která potenciálně umožňuje útočníkovi dostat se k datům, ke kterým nemá daný uživatel systému oprávnění. Řečeno jinak: „útočník“ se může z jedné virtuální mašiny dostat k datům v paměti jiné virtuální mašiny. Problém se týká v podstatě všech CPU z posledních generací u Intelu, což mimo jiné znamená, že z něj plyne i teoretická napadnutelnost všech cloudových služeb využívajících CPU Intel (například Amazon EC2, Google Compute Engine, Microsoft Azure) či jakýchkoli jiných strojů.

Řešení v softwarové podobě existuje, je na Linuxu implementováno jako Page Table Isolation, ale představuje tak velkou zátěž z hlediska přerušení a systémových volání, že při reálném použití dochází k propadu výkonu CPU o jednotky až desítky procent. Řešení totiž spočívá v tom, že pokud program chce po jádru systému data z jeho paměti, musí nyní (patřičně opatchovaný) kernel nejprve smazat TLB cache.

Jak moc velký problém to je?

Detailní popis chyby není z pochopitelných důvodů zatím k dispozici, ale můžeme usuzovat z několika indicií. Tou první je ticho po pěšině, které se Intel snažil držet, podobně jako u Management Engine. To obvykle není dobré znamení. Tím druhým je, že změny do linuxového jádra připutovaly v

rychlém sledu a dokonce jsou backportovány do starších verzí, včetně LTS.

Úpravy existují i za cenu velké ztráty výkonu, takže je jasné, že bezpečnost (resp. závažnost problému) zde má o hodně vyšší prioritu. A v neposlední řadě s ohledem na to, že od loňského podzimu na věci pracuje i Microsoft pro Windows 10 s NT kernelem, lze to vnímat jako potvrzení hardwarové chyby.

Objevilo se více informací o míře propadu výkonu po aplikaci patchů. Obecně se uvádí propad na úrovni 30 až 35 %, Phoronix provedl vlastní rozsáhlejší měření. Z nich vyplynulo, že kupříkladu hry či komprese videa nejsou prakticky vůbec penalizovány. Nicméně dopady v I/O operacích, kompilačních testech či databázových (PostreSQL) jsou hodně velké.

AMD se to netýká

Důležité pro budoucí vývoj je to, že celý problém není dán návrhem x86 architektury jako takové (či nějaké pozdější instrukční sady x86 procesorů), ale konkrétní implementací konkrétní funkcionality tak, jak ji Intel ve svých CPU realizoval. Konkurenční AMD je tedy z obliga, jejích CPU se problém netýká, a platí to jak pro serverové Opterony, tak obecně pro procesory architektur Ryzen, Threadripper a EPYC.

Pikantní ale je, že patche na tuto chybu mají velký výkonnostní dopad i na strojích s AMD CPU. Za vše totiž může aktivace `X86_BUG_CPU_INSECURE`, která vede k použití kódu, který neustále maže TLB. Toto označení je nyní aktivní pro všechny x86 CPU jako bezpečnostní opatření. AMD již řeší jeho odstranění pro svá CPU.

Souvislosti a důsledky budou zajímavé

Dovolte mi nyní volněji dosadit celou věc do souvislostí. Máme zde tedy nyní procesory Intel, u kterých se pro několik posledních generací ví o dvou velkých problémech. Těmi generacemi myslím cokoli od Sandy Bridge výše (o Core 2 se už nemá smysl příliš bavit). V různých verzích x86 CPU architektur Intelu se nachází různé verze Intel Management Engine, tedy vlastní malý běžící „počítač“, aktuálně používající x86 CPU s OS Minix – to samo o sobě je potenciálně velký problém, nicméně probrali jsme ho před časem v samostatném článku.

Intel si zkrátka loni svoji reputaci vůbec nevylepšil a nepřispívá tomu ani neustálé odkládání nových výrobních procesů (indikující neschopnost přivést 10nm výrobu x86 CPU k světu – a dokládají to i nejnovější neoficiální data). A nyní přichází další rána: všechny x86 procesory Intel jsou prokazatelně nebezpečné a není možné s tím nic udělat bez velké výkonnostní penalizace.

A právě ta penalizace je věc, která Intelu dle mého ubírá obchody (vysvětlím za chvíli). Penalizaci na úrovni desítek procent si Intel mohl dovolit v době, kdy neměl konkurenci, tj. kdy AMD měla na trhu mizerné procesory typu Bulldozer/Piledriver (AMD FX 8 a 9). Nyní je situace zcela jiná, AMD má na

trhu vynikající procesory od desktopů (Ryzen), přes hi-end desktopy (Threadripper) až po servery (EPYC). Intel prakticky není schopen jí konkurovat, maximálně dokáže oproti 16jádrovéhu Threadripperu s cenovkou 25 tisíc Kč postavit o trošku výkonnější 18jádrové Core i9–7980XE s cenovkou 48 tisíc Kč.

Sousloví „o trošku výkonnější“ si ale můžeme dnes škrtnout, protože záplaty na hardwarovou chybu v procesorech Intel ubírají výrazně výkon jak na Linuxu, tak na Windows a není v moci Intelu s tím cokoli udělat (avšak nutno zdůraznit, že se to týká spíše určitých typů aplikací). Pokud tuto argumentaci přeženu, tak by na základě známých skutečností mělo být možné tvrdit, že AMD má momentálně na desktopovém trhu prokazatelně rychlejší procesor (Threadripper 1950X) za zhruba poloviční cenu oproti konkurenčnímu model Core i9–7980XE. A podobné lze tvrdit i o serverových procesorech, kde jsou cenové rozdíly mnohdy ještě zajímavější.

Pokud byl rok 2017 z hlediska trhu x86 CPU první po letech stagnace opravdu zajímavým rokem, tak to byl teprve slaboučký odvar toho, co nás čeká letos. Už několik let tvrdím, že Intel usnul na vavřínech, stačilo mu oproti skomírající AMD pouze udržovat status quo a inovovat jen mírně. Nyní to za svůj přístup schytá a může si za to vlastně sám.

Dlužno připomenout, že tento problém s implementací TLB cache není první. V roce 2008 měly první AMD Phenomy též chybu v této části CPU a záplata vedla též k propadům výkonu. Z hlediska architektury x86 CPU tomu tam asi bude u TLB vždy.