Meltdown

chyba umožnující zjistit obsah paměti (včetně systémových procesů)

- spekulativní provádění instrukcí – není (v procesorech intel) vázáno kontrolou oprávnění přístupu

- v okamžiku zjištení neoprávněnosti je spekulativní kód „zahozen“

- ale: spekulativní provedení může mít vedlejší efekt

příklad: if <podm> {promena = load memory (adresa)} ;

kde <podm> je založna na datech v oblasti bez oprávnění přístupu – která je vyhodnocena a spekulativně je proveden príkaz load – po zjištění neoprávněného přístupu se výsledky zahodí, ale – v cache jsou či nejsou načtená data (ke kterým práva máme) na základě podmínky. Přítomnost dat v cache můžeme otestovat.

Řešení: změna ve správě paměti systémových funkcí, KPTI (kernel page table isolation) (update OS)

Spectre

chyba umožnující spustit (spekulativně) libovolný kód → I zjistit obsah paměti (včetně systémových procesů)

- predikce skoků obsahuje informaci kam se skáče – prediktory nerozlisují mezi kódem jádra a uživatelským kódem, rozhoduje se na základě adresy – lze natrénovat prediktor tak že skočí na libolné místo kde jsou pak spekulativně prováděny instrukce.

- Problém zejména u Virtuálních serverů kdy je možné pomocí tohoto exploitu přistoupit (zjistit data) jiného virt.stroje

Řešení: úprava na úrovni mikrokódu, nové instrukce pro vymazání stavu prediktoru (tj. aby bylo možné (na úrovni OS) zajistit ze prediktor jednoho vlákna nebude neovliňovat jiné)

ZombieLoad, RIDL, Fallout

(itntel označuje tuto skupinu jako MDS = microarchitectural data sampling)

- explotity z rodiny Meltdown, postihuje intel.

- umožnují získat data z paměti

- RIDL používá bufferu procesoru Line-Fill, Load Ports

- FallOut používá storage buffer

Řešení: vypnout HT (hyperthreading) (?)