Sicherheitslücke in AMDs Zen-Prozessoren

Experten der TU Dresden demonstrieren einen Seitenkanalangriff vom „Meltdown"-Typ bei Epyc- und Ryzen-CPUs.

AMD hat Untersuchungen von zwei Sicherheitsforschern bestätigt, laut denen ein Software-Thread unter speziellen Umständen vermeintlich geschützte Daten eines anderen Threads aus dem L1D-Cache erbeuten kann, sofern beide auf demselben CPU-Kern laufen. Die Sicherheitslücke wurde unter CVE-2020-12965 als „mittelschwer" (Medium, BSI: Risikostufe 3) eingestuft.

Als Schutz gegen den Angriff genügen Anpassungen des Programmcodes etwa mit „LFENCE"-Anweisungen, die auch gegen die 2019 bei Intel-Prozessoren enttarnte Sicherheitslücke ZombieLoad alias Microarchitectural Data Sampling (MDS) helfen. AMD selbst plant keine Updates zum Schutz gegen diese Sicherheitslücke, also weder Firmware- noch Microcode-Updates sowie auch keine neuen CPU-Versionen.

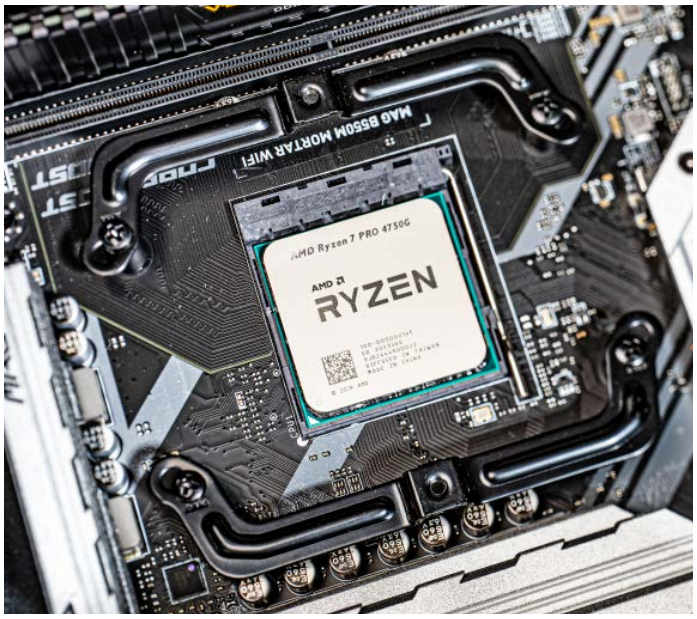
Saidgani Musaev und Christof Fetzer von der TU Dresden schreiben in ihrem Paper (siehe ct.de/ybjk) selbst, dass die „Transient Execution of Non-Canonical Accesses" genannte Seitenkanalattacke für sich genommen kein hohes Risiko darstelle. Sie könne aber in Kombination mit anderen Angriffen deren Wirkung verstärken und belegt, dass derartige Angriffe auch bei AMD-Prozessoren mit „Zen"-Mikroarchitektur funktionieren – anders als bisher angenommen.

Musaev und Fetcher selbst haben nur Prozessoren mit den Zen-Generationen Zen+ (Ryzen 7 2700X und Ryzen Threadripper 2990WX) sowie Zen 2 (Epyc 7262) erfolgreich attackiert. Betroffen sind aber laut Musaev nach Einschätzung von AMD auch alle anderen Ryzen- und Epyc-Varianten sowie Athlons mit Zen-Technik, auch die aktuellen Ryzens und Epycs mit Zen 3.

Der Angriff funktioniert auch bei jenen älteren Intel-Prozessoren, die gegen MDS empfindlich sind, was die Sicherheitsforscher aber auch erwartet hatten. Ein Core i7-10510U (Comet Lake) erwies sich hingegen als unempfindlich.

(ciw@ct.de)

Transient Execution of Non-Canonical Accesses: ***ct.de/ybjk***



AMD-Prozessoren mit Zen-Mikroarchitektur wie dieser Ryzen 7 Pro 4750G sind durch „Transient Execution of Non-Canonical Accesses" angreifbar.