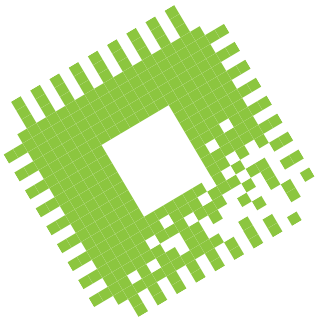
Bit-Rauschen

CPU-Sicherheitslücken und Cloud-Marktkonzentration



Trotz des „Security First“-Versprechens verhaspelt sich Intel beim Stopfen von Sicherheitslücken. Das Geld fließt weiter in Strömen, weil Cloud-Giganten immer mehr Milliarden verteilen.

Von Christof Windeck

Mit der Veröffentlichung von mehr als 70 Sicherheitslücken hat sich Intel am 12. November einigen Ärger eingehandelt. Ein gewisses Murren begleitete schon ältere CPU-Bugs wie Spectre und L1TF, als Sicherheitsexperten Intels monatelange Geheimhaltungsfristen kritisierten. Diesmal gab es öffentliche Vorwürfe via Twitter und New York Times: Demnach weiß Intel schon seit über einem Jahr Bescheid über Zombieload v2 alias TSX Asynchronous Abort (TAA). Schlimmer noch: Der endlich fertiggestellte Patch schütze nicht einmal vollständig. Zudem hatte Intel zwischenzeitlich die zweite Xeon-SP-Generation Cascade Lake vorgestellt, ohne ein Sterbenswörtchen über TAA zu verlieren.

Doch was hätte Intels Verkaufsteam sagen sollen? Etwa „kaufen Sie unseren neuen Xeon, weil er ein bisschen langsamer und teurer als der AMD Epyc 7002 ist, dafür aber die TAA-Lücke hat“? Aber selbst wenn die Arbeit am Patch tatsächlich über ein Jahr lang dauerte, wirft das kein gutes Licht auf Intel. Zumal es das Konzept der koordinierten Veröffentlichung ad absurdum führt, wenn am Ende der vereinbarten Geheimhaltungsfrist doch kein vollständiger Patch bereitsteht.

Zwar hat Intel die Sicherheitsabteilung gestärkt und die Mehrzahl der über 70 Sicherheitslücken in internen Labors gefunden. Doch hatte man nach dem feierlichen „Sicherheit zuerst!“-Versprechen von Anfang 2018 mehr erwartet. Aber das kam vielleicht auch eher vom Verkaufsteam, schließlich musste man wenige Tage nach dem Spectre-Schock irgendwas sagen. Und bestimmt war es Zufall, dass Intel zahlreiche IT-Journalisten just am Tag der Veröffentlichung der Bug-Liste zum nahezu ereignislosen „KI-Gipfel“ einlud. Dort berichtete die Nervana-Sparte zum x-ten Mal über die KI-Beschleuniger NNP-T1000 und NNP-I1000, ohne Preise und Termine zu verraten. Immerhin will die Movidius-Abteilung drei Jahre nach dem Myriad X 2020 einen Nachfolger bringen.

Ganz so schlimm, wie es die von Intel genervten Sicherheitsexperten von VUSec darstellen, ist die Sicherheitslücke TAA aber wiederum auch nicht. Letztlich trifft sie nur einige Datenbank-Server. Denn die schwere Lücke klafft nur in den Transactional Synchronization Extensions (TSX) des Prozessors. Sofern es nicht um Datenbank-Software mit TSX geht, kann man es schadlos abschalten, dank Microcode-Update etwa auch per Linux-Bootoption oder Windows-Registry.

Intel wirkt mit der Fülle an Sicherheitslücken überfordert, wie auch „TPM-Fail“ zeigt (siehe S. 57): Das von Microsoft für PCs mit Windows-Logo erzwungene Trusted Platform Module 2.0 (TPM 2.0) soll die Sicherheit stärken. Flugs baute Intel ein Firmware-TPM (fTPM) in die Management Engine (ME) ein, die man mittlerweile Converged and Security Management Engine (CSME) nennt. Das fTPM steckt bei Core-i-Chips in der „Platform Trust Technology“ (PTT), die Teil von ME beziehungsweise CSME ist. Am 12. November hat Intel nun zwar den TPM-Bug veröffentlicht, wirft dabei aber Begriffe wie PTT, ME und CSME munter durcheinander und hat noch nicht einmal für alle Mini-PCs der eigenen NUC-Familie die BIOS-Updates fertig.

Marktkonzentrate

Wie schon im letzten Bit-Rauschen erwähnt, verdient Intel trotz aller Pannen haufenweise Geld. Da stört es auch wenig, dass AMDs neuer 16-Kern-Ryzen (siehe S. 48) sogar Intels Core X abhängt. Doch zu Intels Glück legen nicht nur Notebooks zu, sondern – anders als noch im Frühjahr erwartet – auch die Rechenzentren. 2019 will Google laut Hausblog 13 Milliarden Dollar in den USA investieren, zählt hier aber den Bau von vier neuen Rechenzentren und von Solar- und Windkraftanlagen mit. 2018 hatte alleine Google weltweit mehr als 10 Milliarden US-Dollar in die Aufrüstung seiner Cloud-Flotte gesteckt, melden die Marktforscher von Intersect360. Auch Amazon pumpte 2018 mehr als 5 Milliarden US-Dollar in Server – 82 Prozent der weltweiten Cloud-Investitionen verteilen sich auf lediglich elf Firmen. Die Marktmacht dieses Hyperscaler-Oligopols wächst immer weiter, weil sie Möglichkeiten haben, die kleineren Firmen verschlossen sind, etwa gewaltige Datenmassen für die KI-Enwticklung.

Auch in anderen Ecken des IT-Marktes gibt es Giganten: Beispielsweise ist Apple der größte Einzelkunde des Auftragsfertigers TSMC und sorgte 2018 für 22 Prozent des Umsatzes dort von 34 Milliarden US-Dollar. Mit weniger als 10 Prozent folgt Huawei auf Platz zwei – nur zehn Kunden sorgen bei TSMC für 68 Prozent des Umsatzes, das restliche Drittel verteilt sich auf fast 500 Firmen. *(ciw@ct.de)* c't

Den Xeon-SP „Cascade Lake“ lieferte Intel inklusive TAA-Sicherheitslücke aus, so der Vorwurf von VUSec.