Die Riesenlücken

Sicherheitslücken in den meisten modernen Prozessoren

Unter den Namen „Meltdown“ und „Spectre“ wurden Anfang Januar gravierende Sicherheitslücken in Prozessoren von Intel, AMD und vielen anderen Herstellern bekannt. Um sie zu schließen, erscheinen Updates für die meisten aktuellen Betriebssysteme, für Browser und andere Software. So schützen Sie Ihre Computer und Smartphones.

Von Christof Windeck

Es ist eine Katastrophe für die Hersteller von Prozessoren, Betriebssystemen, Browsern, Computern, Servern und Smartphones: Sicherheitsforscher haben drei kritische Lücken in den meisten aktuellen Intel-Prozessoren ausgemacht; zwei betreffen auch die von AMD sowie einige mit ARM-, POWER- und SPARC-Mikroarchitektur. Die Sicherheitslücken ermöglichen es, vermeintlich gut geschützte Daten wie Passwörter aus dem RAM auszulesen. Deshalb erscheinen zurzeit zahlreiche Updates für Betriebssysteme (Windows, macOS, Linux, iOS, Android, FreeBSD und so weiter), Browser, NAS-Speicherboxen, Grafiktreiber und manche Anwendungen. Wir raten dringend dazu, diese Updates bald einzuspielen, und beschreiben auf den folgenden Seiten die Vorgehensweisen für unterschiedliche Systeme. Außerdem erklären wir, was es mit den Sicherheitslücken auf sich hat.

Loch im RAM-Zaun

Die Entdecker der Lücken haben sie Meltdown und Spectre getauft; das bedeutet so viel wie (Kern-)Schmelze und Phantom, Schreckgespenst. Es geht um drei Angriffsmöglichkeiten (siehe Tabelle), die sich ungefähr so beschreiben lassen: Eine laufende Anwendung kann RAM-Inhalte auslesen, auf die sie eigentlich keinen Zugriff haben sollte. Meltdown und Spectre hebeln die bisher als zuverlässig angenommene Trennung von RAM-Bereichen aus – allerdings auf Umwegen, etwa über Caches. Man spricht daher von Seitenkanalangriffen (Side Channel Attacks).

Die gegenseitige Abschottung von Speicherbereichen ist ein Grundpfeiler der IT-Sicherheit, wie ein einfaches Beispiel zeigt: Passwort-Speicherfunktionen von Browsern wären extrem unsicher, wenn ein anderer laufender Prozess einfach nach Belieben sämtliche Daten im Hauptspeicher (RAM) lesen könnte. Besonders hart treffen die Lücken Cloud-Rechenzenten, in denen virtuelle Maschinen Daten unterschiedlicher Kunden auf demselben Server verarbeiten.

Meltdown und Spectre missbrauchen Funktionen, die in Milliarden von Prozessoren stecken: Out-of-Order-Execution (OoOE), Speculative Execution und Branch Prediction. Intel hat OoOE vor rund zwanzig Jahren mit dem Pentium Pro eingeführt: Falls der Prozessor mit der Ausführung eines Befehls warten muss, etwa auf Daten aus dem RAM, verarbeitet er schon einmal einen anderen Befehl, der eigentlich erst später an der Reihe wäre. Er arbeitet Code also nicht in der Reihenfolge ab, wie sie im Programm steht (In Order), sondern in einer anderen, optimierten: Out of Order.

Programmcode enthält außerdem Bedingungen, durch die sich der Ablauf verzweigt (Branching). Sprungvorhersageeinheiten versuchen, die vermutlich als Nächstes wichtigen Speicheradressen zu erraten (Branch Prediction). Falls Ressourcen frei sind, führt die CPU Befehle schon einmal auf Verdacht aus (Speculative Execution), obwohl sie vielleicht doch nicht nötig sind – dann werden die Resultate verworfen. Doch unter anderem dank KI-Algorithmen wie neuronalen Netzen erzielen moderne Sprungvorhersageeinheiten hohe Trefferraten und steigern die Rechenleistung erheblich. Würde man OoOE, Branch Prediction und Speculative Execution abschalten, um Sicherheitslücken zu schließen, würde die Performance drastisch sinken.

Brems-Patches

Doch auch einige der nun verteilten Updates mindern die Systemleistung. Das räumen Microsoft und Intel ein. Es hängt aber von vielen Faktoren ab, wie stark die Bremswirkung ausfällt und ob man sie bei der Arbeit am PC spürt.

Zum Schließen der Meltdown-Lücke, von der nur Intel-Prozessoren betroffen sind, sind tiefgreifende Änderungen am Kernel des Betriebssystems nötig. Sie trennen die Speicher-Adressbereiche des privilegierten Betriebssystem-Kernels gründlicher von denen laufender Programme im sogenannten „User Space“. Die Technik nennt man auch Page Table Isolation (PTI). Jüngere Intel-Prozessoren ab der vierten Core-i-Generation (Haswell, Core i-4000, Xeon E5 v3) beherrschen eine Funktion namens Process-Context Identifier (PCID). Diese reduziert Leistungseinbußen durch PTI. Anders gesagt: Bei älteren (vor 2013) und schwächeren Prozessoren bremsen die Sicherheitsupdates stärker als bei modernen. Nach

BIOS-Updates für Intel-Systeme

Gegen die Sicherheitslücke Branch Target Injection (BTI, Spectre Variante 2) gibt es zwei Schutzverfahren. Beide erfordern bei Intel-Systemen ein Zusammenspiel von Updates des Betriebssystems mit CPU-Microcode-Updates, die neue Funktionen der Prozessoren nachrüsten.

Das erste BTI-Schutzverfahren verwendet drei neue CPU-Befehle: Indirect Branch Restricted Speculation (IBRS), Single Thread Indirect Branch Predictors (STIBP) und Indirect Branch Predictor Barrier (IBPB). Sie sollen auch in alle Prozessoren kommender Generationen eingebaut werden. Die Dokumentation will Intel in einer künftigen Revision des Entwicklerleitfadens „Intel 64 and IA-32 Architectures Software Developer’s Manual“ nachreichen.

Bei der zweiten BTI-Schutztechnik ersetzen Programmierer bestimmte Sprungbefehle durch ein Konzept namens „Return Trampoline“ (Retpoline). Das funktioniert bei Intel-Prozessoren ab der Generation Broadwell (Core i-5000, Xeon E5 v4) wiederum erst nach einem Microcode-Update.

Die CPU-Sicherheitslücken Meltdown und Spectre

Google-Name	Kurzbezeichnung	CVE-Nummer	betroffene Prozessoren und jeweilige Patches			
			Intel	AMD	ARM[1]	IBM POWER
Spectre, Variante 1	Bounds Check Bypass	CVE-2017-5753	✓ (A, B)	✓ (A, B)	✓ (A, B)	✓ (A)
Spectre, Variante 2	Branch Target Injection (BTI)	CVE-2017-5715	✓ (A, B, C)	✓ (A, C[2])	✓ (A)	✓ (A, C[3])
Meltdown	Rogue Data Cache Load	CVE-2017-5754	✓ (D)	–	✓[4]	–

A: Updates für Betriebssystem und mitgelieferte Browser (IE, Edge, WebKit) vom Hersteller des Betriebsssystems
B: Updates von separaten Anwendung(en), Browsern, Virenscannern und/oder Treibern von den jeweiligen Herstellern
C: CPU-Microcode-Update, bei Windows via BIOS-Update, bei vielen Linuxen via Distributions-Update
D: Update für Betriebssystem (PTI); Prozessoren ab Haswell (Core i-4000/Xeon E5 v3) reduzieren PTI-Bremswirkung mit PCID

[1] betroffen sind Cortex-A8, -A9, -A15, -A17, -A57, -A72, -A73, -A57, -R7, -R8, also etwa nicht der Cortex-A53 im Raspi
[2] laut AMD nur geringes Risiko „nahe Null“, trotzdem „optionale“ Microcode-Updates für Ryzen/Epyc, später für ältere Prozessoren
[3] Firmware-Update für POWER7+, POWER8, POWER9
[4] nur Cortex-A75, der noch nicht in einem Chip erschienen ist

bisherigem Kenntnisstand sinkt die Leistung typisch genutzter Desktop-PCs, Notebooks und Tablets mit Windows 10 und aktuellen Prozessoren nur im einstelligen Prozentbereich; das ist kaum spürbar. Merkliche Einbußen erwartet Microsoft bei Windows-7-PCs mit älteren Prozessoren. Wir konnten hingegen in mehreren Benchmark-Tests mit älteren Windows-7-Systemen keinen nennenswerten Leistungsabfall messen.

Die stärkste Auswirkung gibt es bei Systemen mit Intel-Prozessoren und schnellen SSDs, insbesondere mit teuren PCI-Express-(PCIe-)SSDs mit NVMe-Protokoll. Die Auswirkungen zeigen sich erst, wenn außer dem Windows-Update auch das Microcode-Update (siehe Kasten) eingespielt ist. Sequenzielle Datentransfers werden zwar kaum beeinträchtigt, das Kopieren größerer Dateien läuft praktisch ebenso schnell wie vorher. Doch zufällig verteilte Zugriffe auf kleine Datenblöcke brechen in manchen – nicht allen! – Szenarien um bis zu 50 Prozent ein. Es gibt Berichte, laut denen das Booten von Windows nach dem Patch länger dauert, weil die SSD-Performance sinkt.

Die IO-Bremswirkung sorgt dafür, dass auch der Anwendungsbenchmark BAPCo SYSmark 2014 auf manchen Systemen mit Intel-Prozessor bis zu 10 Prozent weniger Punkte liefert. Das geht dann besonders auf den „Responsiveness“-Test des Benchmarks zurück, der die SSD belastet.

Bei der Arbeit am PC spürt man die IOPS-Einbußen der NVMe-SSDs freilich kaum, weil sie typische Desktop-Software im Vergleich zu den langsameren SATA-SSDs nur in Sonderfällen beschleunigen. Auf SATA-SSDs wirkt sich der Patch wiederum kaum aus, Magnetfestplatten sind wohl nicht messbar betroffen. Bei Systemen mit AMD-Prozessoren sinken die IOPS-Werte von NVMe-SSDs viel weniger ab, wir konnten maximal 6 Prozent messen.

Denkbar ist, dass sich die IO-Nachteile auch bei Anwendungen bemerkbar machen, die isochrone Transfers benötigen, etwa bei Audio-Software. Wir kennen dazu bisher aber keine Beispiele.

3D-Spiele zeigen wohl nur in Ausnahmefällen spürbare Einbußen; bei unseren Messungen konnten wir jedenfalls nur minimale Abweichungen feststellen. Während die gemittelten Bildwiederholraten kaum sinken, sacken in manchen Spielen jedoch die niedrigsten Wiederholraten noch etwas weiter ab.

Deutlicher sind die Auswirkungen auf manche Server-Anwendungen. Pauschale Aussagen sind wegen der vielen unterschiedlichen Server-Anwendungen kaum möglich. Aber IOPS-Rückgänge bei SSD-Zugriffen können etwa Datenbanken stark bremsen. Falls der Ressourcenbedarf bei Servern steigt, kann das zu Engpässen bei der Leistung, zu mehr Stromverbrauch und bei Nutzern von Cloud-Diensten zu höheren Kosten führen. Microsoft rät dazu, bei hoch belasteten Windows-Servern abzuwägen, ob der Patch nötig ist, etwa weil außer der Server-Anwendung keine fremde Software läuft und andere Sicherheitssysteme wie Firewalls greifen. Es ist zu hoffen, dass Performance-Einbußen nach optimierten Updates wieder abnehmen.

Nicht betroffen

Konkrete Angriffe per Meltdown und Spectre sind uns bisher nicht bekannt, sie löschen oder verschlüsseln zudem keine Daten. Die Lücken lassen sich auch nicht für Remote-Angriffe via Ethernet oder WLAN nutzen, weil der Schadcode auf dem angegriffenen System selbst laufen muss. Deshalb sind viele Embedded Systems und Router nicht direkt angreifbar. Über sonstige Lücken lassen sich Meltdown und Spectre womöglich jedoch nut-

Leistungseinbußen durch Windows- und BIOS-Updates gegen Meltdown & Spectre

System	Patches	Intel Core i-8700K	AMD Ryzen 7 1700X	Intel Core 7-4770
Erscheinungsjahr		2017	2017	2013
BIOS-(Microcode-)Update		mit	nicht verfügbar	nicht verfügbar
Cinebench R15 single/multi [Punkte]	ohne	203/1412	156/1546	156/748
Cinebench R15 single/multi [Punkte])	**mit**	202/1403	153/1542	155/749
7-zip [MIPS]	ohne	38430	39384	22625
7-zip [MIPS]	**mit**	39043	38881	22140
BAPCo SYSmark 2014 SE [Punkte]	ohne	1808	1363	1290
BAPCo SYSmark 2014 SE [Punkte]	**mit**	1723	1350	1264
SYSmark Responsiveness [Punkte]	ohne	1431	1052	1200
SYSmark Responsiveness [Punkte]	**mit**	1331	1038	1155
PC Mark 10 [Punkte]	ohne	4806	5259	3521
PC Mark 10 [Punkte]	**mit**	4733	5263	3470
PCIe-SSD, 1 Worker [IOPS]	ohne	168045/197949	70086/104433	109400/136347
PCIe-SSD, 1 Worker [IOPS]	**mit**	79313/105986	69268/98355	113669/147040
PCIe-SSD, n Worker [IOPS]	ohne	377282/336000	377000/335000	374489/334891
PCIe-SSD, n Worker [IOPS]	**mit**	374040/335150	376000/335000	374895/335287
PCIe-SSD, sequenziell [MByte/s]	ohne	2121/3347	2129/3567	2137/3184
PCIe-SSD, sequenziell [MByte/s]	**mit**	2136/3516	2123/3564	2110/3181
SATA-SSD [IOPS]	ohne	89556/98673	92350/97660	90885/98232
SATA-SSD [IOPS]	**mit**	88624/98864	91779/95797	91023/98508
SATA-SSD, sequenziell [MByte/s]	ohne	504/560	527/562	526/562
SATA-SSD, sequenziell [MByte/s]	**mit**	522/560	526/562	526/563

zen, um größeren Schaden anzurichten. Computer und Smartphones mit Prozessoren, die mit In-Order-Execution ohne spekulative Ausführung arbeiten, sind von Meltdown und Spectre nicht betroffen. Das gilt etwa für alle Raspberry Pi. Selbst der 64-bittige ARM Cortex-A53 im Raspi 3 ist unkritisch – und diese Kerne stecken auch im Qualcomm Snapdragon 410, der Smartphones wie das Motorola Moto G3 antreibt. Einige ältere Intel-Atom-Typen wie der N270 arbeiten auch In Order.

Geräte mit AMD-Prozessoren sind zwar von den Spectre-Lücken betroffen, aber laut AMD genügen Updates von Betriebssystem und Software zum Schutz. Trotzdem will AMD „optionale" Microcode-Updates liefern. Welcher Prozessor in Ihrem PC steckt, finden Sie unter Windows beispielsweise mit CPU-Z heraus (ct.de/yd7r). Der Link führt auch zu Seiten bei heise online, die wiederum zu Listen mit betroffenen Prozessoren und zu Update- und Info-Seiten von Herstellern führen.

Linderung statt Heilung

Intel, Microsoft und die Entdecker der Lücken sprechen interessanterweise nicht davon, die Sicherheitslücken zu schließen. Stattdessen verwenden sie durchweg den englischen Begriff „Mitigation", der so viel bedeutet wie Abschwächung oder Linderung. Die Spectre-Entdecker vermuten, dass noch weitere Schwachstellen in den erwähnten CPU-Funktionen schlummern, und sie erwarten, dass sich die Lücken erst mit künftigen, in der Hardware veränderten Prozessoren ganz schließen lassen werden. Intel will etwa die sogenannte Control Flow Enforcement Technology (CET) einbauen, um den Schutz gegen Branch Target Injection (BTI, Spectre Variante 2) zu verbessern. Wann solche Chips erscheinen, weiß derzeit niemand – das dauert wohl mehrere Monate, vielleicht Jahre.

Für 32-Bit-x86-Betriebssysteme sind derzeit keine Updates verfügbar. Bei aktuellen Intel-Systemen lässt sich BTI nur dann erschweren, wenn der Prozessor ein sogenanntes Microcode-Update erhält. Es rüstet drei neue Funktionen nach (siehe Kasten auf S. 59). Dieses Update will Intel zuerst für Prozessoren liefern, die seit 2013 ausgeliefert wurden. Wie es mit älteren Core-i-Prozessoren weitergeht, ist unklar, auch weil es vom jeweiligen Systemhersteller abhängt: Der muss die Microcode-Updates in neue BIOS-Versionen einfügen, die er dann als BIOS-Updates ausliefert. Die muss der Besitzer des PCs, Notebooks, Servers oder Mainboards dann einspielen. Linux-Nutzer sind etwas besser dran: Viele Distributionen bringen CPU-Microcode-Updates automatisch. Wieso das unter Windows 10 nicht klappt, ist derzeit unklar. Als wäre das nicht schon ärgerlich genug, haben erst wenige Hersteller von PCs und Mainboards überhaupt schon BIOS-Updates fertig.

Browser, Programme, Treiber

Besonders bedrohlich sind die Spectre-Lücken für Software, die einerseits Daten aus dem Internet lädt und andererseits sensible Informationen verarbeitet. Das gilt vor allem für Browser: Sie laden ausführbaren Code wie JavaScript und HTML5 von Webseiten und senden Passwörter – oder speichern sie sogar. Daher enthalten die Updates für Windows und macOS auch Updates für die integrierten Browser. Wer Chrome, Firefox oder andere Browser nutzt, muss auch hier auf Updates achten. Den Schutz verstärken Skriptblocker wie NoScript.

Aktualisierungen gibt es auch für manche Treiber, etwa für GeForce-Grafikkarten von Nvidia, aber nur für wenige Anwendungsprogramme. Wir haben unter anderem Hersteller von Banking-Software dazu befragt. Sowohl Buhl Data als auch Star Finanz antworteten, dass sie keine Schwachstellen befürchten, sofern alle Windows-Updates eingespielt würden.

Service-Katastrophe

Intel, Microsoft und viele Smartphone-Hersteller versagen beim Krisenmanagement. Zwar gibt es Updates, aber die Dokumentation ist ungenügend und Besitzer älterer Geräte erhalten zu wenig konkrete Informationen. In den USA gibt es die ersten Klagen gegen Intel. Wie die Rechte europäischer Verbraucher sind, deren Geräte nach Ablauf von Gewährleistung und Garantie Sicherheitslücken aufweisen, ist schwer einzuschätzen. Das zeigen auch die Prozesse gegen Volkswagen wegen Betrugs bei der Abgasreinigung. Besseren Verbraucherschutz müsste die Politik durchsetzen, tut es aber nicht.

Meltdown und Spectre werden die IT-Branche noch eine Weile beschäftigen. Wann erste Prozessoren ohne diese Fehler erscheinen, lässt sich derzeit nicht einschätzen; es kann jedenfalls mehrere Monate dauern. *(ciw@ct.de)* c't

Download CPU-Z, Update-Listen:
ct.de/yd7r

Glossar

Im Zuge der Berichterstattung über Meltdown und Spectre tauchen viele Abkürzungen auf.

ASLR: Address Space Layout Randomization. Zufällige Adresszuweisung für Programme zur Laufzeit, um Angriffe auf Speicheradressen zu erschweren.

BTI: Branch Target Injection. Angriff durch Manipulation der CPU-Sprungvorhersage.

CVE: Common Vulnerabilities and Exposures. Öffentliche Liste von IT-Sicherheitslücken.

Exploit: Ausnutzung einer Sicherheitslücke.

KASLR: Kernel Address Space Layout Randomization. ASLR für den Kernel.

KAISER: Kernel Address Isolation to have Side Channels Efficiently Removed. Ein Vorläufer von PTI.

KPTI: Kernel Page Table Isolation. Synonym für PTI.

KVA: Kernel Virtual Address (Space). Speicher-Adressraum des (Windows-) Kernels, hier eher gemeint im Sinne von PTI.

KVA Shadowing: Mapping von Teilen des KVA in den User Address Space.

PCID: Process-Context Identifiers. Funktion der CPU, die PTI beschleunigt.

PoC: Proof of Concept. Demonstration, etwa eines Software-Angriffs.

PTI: Page Table Isolation. Gründlichere Trennung der virtuellen Speicher-Adressbereiche von Kernel- und User-Space.

Zero Day: Tag Null. Gemeint ist eine bisher öffentlich unbekannte Sicherheitslücke, für die es noch keinen Patch gibt. Solche Lücken sind für Angreifer besonders wertvoll und das Wissen darüber wird sogar verkauft.