Der Spectre-Schock

Ein Jahr nach Spectre und Meltdown: AMD und Intel immer noch im Halbschlaf

Spectre und Meltdown belegten Anfang 2018, dass aktuelle Prozessoren für Server, PCs und Notebooks fundamental unsicher sind. Nach einem Jahr sind die Sicherheitslücken zwar geflickt, aber nicht beseitigt.

Von Christof Windeck

Es gibt zwei entgegengesetzte Blickwinkel auf die Sicherheitslücken Spectre und Meltdown: „Alles halb so schlimm“ oder „Katastrophe ohne Ende“. Für beide Sichtweisen gibt es gute Argumente. Im Wesentlichen hängt die Bewertung aber davon ab, ob man einen PC oder ein Notebook als persönliches Arbeits- oder Spielgerät nutzt oder ob man ein Cloud-Rechenzentrum betreibt.

Die Experten, die Mitte 2017 ihre Entdeckungen an Intel, AMD, IBM und ARM meldeten, legten ihre Finger in eine Wunde: Die leistungssteigernden Prozessorfunktionen Sprungvorhersage und spekulative Ausführung reißen in ihren bisher umgesetzten Versionen tief reichende Sicherheitslücken auf. Und die Probleme wurden innerhalb der vergangenen 18 Monate nur eingedämmt, aber nicht grundsätzlich gelöst. Schlimmer noch: Neue Varianten von Spectre-Attacken tauchten auf.

Die meisten davon lassen sich durch Schutzmaßnahmen verhindern, die mittlerweile umgesetzt wurden. Das sind vorwiegend Patches für Betriebssysteme, darunter Windows 10, Linux, macOS und OpenBSD. Außerdem haben AMD und Intel Microcode-Updates erarbeitet.

Betroffene

Im Verlauf des Jahres hat sich die Einschätzung bestätigt, dass Spectre und Meltdown nur bei sehr wenigen „normalen“ PC-Nutzern das Risiko für Malware-Angriffe steigern. Denn erstens wurden die Angriffsmöglichkeiten durch die erwähnten Updates stark eingeschränkt, zweitens sind die Attacken sehr kompliziert, drittens müssen sie für den jeweiligen Prozessor maßgeschneidert sein und viertens lauern auf den meisten Windows-PCs viel einfacher nutzbare Sicherheitslücken. Letzteres zeigen die aktuell wieder einmal grassierenden Erpressungstrojaner wie Emotet. Da wundert es nicht, dass bisher noch keine praktischen Angriffe via Spectre oder Meltdown in freier Wildbahn beobachtet wurden.

Ein großes Problem für die Betreiber von Cloud-Rechenzentren ist hingegen die Spectre-Next-Generation-(Spectre-NG-)Lücke L1 Terminal Fault (L1TF). Denn auf solchen Cloud-Servern laufen zahlreiche virtuelle Maschinen (VMs) gleichzeitig auf demselben Prozessor. Ein Cloud-Nutzer könnte eine bösartige VM aufspielen, die per L1TF Daten aus anderen laufenden VMs stiehlt. L1TF wurde daher als deutlich höheres Sicherheitsrisiko (Stufe „hoch“, Index 7,3) als die anderen Spectre- und Meltdown-Lücken eingestuft („mittel“ mit 4,3 bis 5,6). Doch auch gegen L1TF gibt es bereits Patches und L1TF ist für normale (Windows-)PCs

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

unwesentlich. Einige der Updates gegen die CPU-Lücken reduzieren die Systemperformance. Allerdings ist das nur in Ausnahmefällen spürbar. Manche der zuerst verteilten Patches führten zu Einbrüchen bei I/O-Operationen, etwa bei SSD-Zugriffen auf zufällig verteilte Adressen. Das wurde aber mittlerweile optimiert. Letztlich sind die Performance-Einbußen bei modernen Systemen unwesentlich, bis auf wenige Ausnahmen.

Träge Reaktionen

Auch wenn also das Bedrohungspotenzial von Spectre und Meltdown für durchschnittliche PC-Nutzer sehr gering ist, wünscht man sich fehlerfreie Computer. Davon sind wir aber noch weit entfernt. Denn würde man spekulative Ausführung (speculative execution) und Out-of-Order-Execution einfach abschalten, wären moderne Prozessoren zwar viel sicherer, aber auch viel langsamer.

Im November erschien ein Paper mit systematischen Untersuchungen bereits bekannter sowie neuer Spectre- und Meltdown-Lücken. An diesem Paper waren einige der ursprünglichen Spectre-Entdecker beteiligt, etwa Michael Schwarz und Daniel Gruss von der TU Graz. Die Autoren werfen den CPU-Herstellern AMD und Intel sowie auch ARM vor, die Bugs nicht ausreichend zu untersuchen. Sie haben sieben neue Angriffsmöglichkeiten gefunden, die an der grundsätzlichen Situation allerdings nichts ändern – es war beispielsweise kein Fehler darunter, der so schwerwiegend ist, dass er eine eigene CVE-Nummer bekommt. Interessant ist der Forschungsbeitrag auch, weil er Angriffe vom Spectre-Typ und vom Meltdown-Typ nochmals genauer unterscheidet. Zwar missbrauchen beide Angriffstypen verdeckte Seitenkanäle in der Mikroarchitektur der jeweils betroffenen Prozessoren. Doch (hypothetische) Malware, die Lücken vom Meltdown-Typ ausnutzt, kommt damit an stärker geschützte Daten heran als mit Spectre-Angriffen. Insbesondere erlauben es einige Meltdown-Attacken, die Grenzen zwischen User- und Kernel-Adressraum zu überwinden.

Die Forscher klassifizieren auch einige CPU-Lücken neu. So nennen sie den ursprünglich als Spectre V1.2 (Read-only Protection Bypass) vorgestellten Bug nun Meltdown-RW, weil er im Kern einen Mechanismus vom Meltdown-Typ nutzt, nämlich das Page-Fault-Signal #PF durch schreibenden Zugriff auf einen Read-only markierten Adressbereich, den der Prozess nur lesen dürfte. Und Meltdown-BR ist eng mit Spectre V1.1 verwandt, nutzt aber wiederum nicht eine Spekulationsfunktion, sondern das bewusst provozierte Exception-Signal Bound Range Exceeded (#BR). Laut den Forschern trifft Meltdown-BR auch AMD-Prozessoren.

Wegducken

Es ist bezeichnend, dass AMD auf solche Hinweise noch nicht reagiert hat – dort stellt man sich tot. Auch die bereits im März 2018 aufgedeckten Sicherheitslücken Ryzenfall und Chimera hat AMD zwar bestätigt, aber bisher dazu keine weiteren Informationen herausgerückt.

Intel verhält sich nicht besser, trotz des Versprechens „Security first“ von vor einem Jahr. Vom CPU-Marktführer hört man vor allem schematische Antworten, die vermutlich penibel von der Rechtsabteilung geprüft wurden: Man hat Angst vor Aktienkursverlusten und Klagen.

Man findet auf den Webseiten von AMD und Intel derzeit keine verständlichen Übersichtstabellen, welche Prozessoren von welchen Fehlern betroffen sind. Solche Informationen muss man sich stückchenweise zusammenklauben.

Microcode-Updates

Bei aller Kritik an AMD und Intel: Untätig waren die CPU-Hersteller nicht. Beide arbeiten sowohl an Updates für Altsysteme als auch an Schutzfunktionen für neue Prozessorgenerationen.

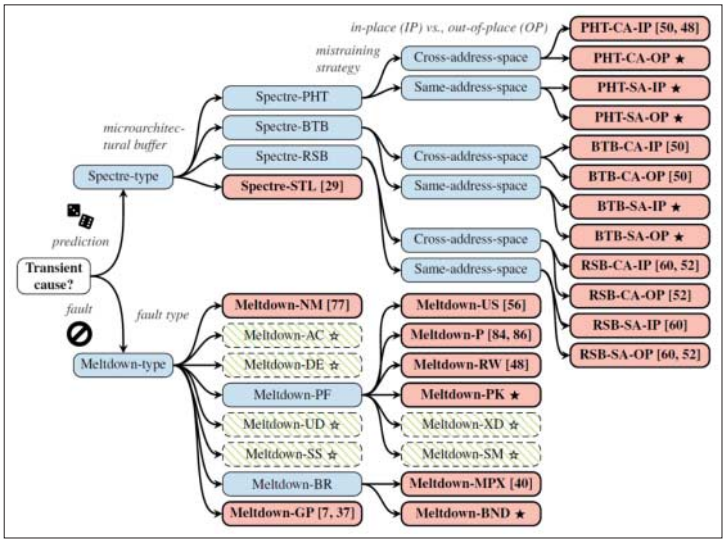
Für den Schutz gegen Spectre V2 benötigen Intel-Prozessoren sogenannte Microcode-Updates; für AMD-Prozessoren sind sie nicht unbedingt nötig, aber empfohlen. Diese Microcode-Updates waren zunächst nur über den Umweg von BIOS-Updates erhältlich. Diese wiederum spielen viele PC-Besitzer nicht ein, außerdem verweigerten viele PC-Hersteller die Erstellung von BIOS-Updates für ältere Rechner. Daher sind Microcode-Updates nun per Windows-Update erhältlich, so wie es zuvor schon bei Linux üblich war – Intel stellt dazu seit Jahren das Linux Processor Microcode Update File bereit. Der Haken daran: Die jüngsten Updates, die auch vor L1TF schützen sollen, bringt Windows Update nicht automatisch ins System.

Mainboards für aktuelle Prozessoren kommen meistens schon mit BIOS-Versionen, die Microcode-Updates gegen Spectre enthalten. Intel hat zudem bei den seit Herbst 2018 ausgelieferten Core-i-9000-Typen schon einige Schutzmaßnahmen eingebaut, hier sind Meltdown (genauer: Meltdown-US) und L1TF kein Thema mehr. Für Spectre V1 ist keine Hardware-Abhilfe geplant, dagegen schützen Updates von Betriebssystemen und Hypervisoren.

Die kommenden AMD-CPUs für Desktop-PCs der Baureihe Ryzen 3000 mit Zen-2-Mikroarchitektur sollen stärker gegen Spectre geschützt sein, die meisten Meltdown-Lücken treffen ohnehin nur Intel-Prozessoren.

Pleiten, Pech und Pannen

AMD und Intel haben beim Stopfen der Sicherheitslücken mehrere schwere Fehler gemacht. So ist es schon peinlich, dass die Veröffentlichung im Januar 2018 nach sechs Monaten Vorlauf letztlich doch unkoordiniert verlief. AMD machte sogar den Eindruck, im Schlaf überrascht worden zu sein, und veröffentlichte zunächst Einschätzungen, die dann wieder zurückgenommen wurden. Schlimmer lief es bei



Eine systematische Analyse möglicher Spectre- und Meltdown-Lücken überlassen die CPU-Hersteller lieber unabhängigen Forschern.

Bild: Claudio Canella et al., TU Graz

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Aktuelle Prozessoren: Meltdown und Spectre

Sicherheitslücke	Spectre V1	Spectre V2	Meltdown	L1TF
CPU-Typ	betroffen / Abhilfe	betroffen / Abhilfe	betroffen / Abhilfe	betroffen / Abhilfe
AMD Ryzen 2000	✓ / Betriebssystem	✓ / Betriebssyst. u. MCU[1]	– (nur Meltdown-BR) / k. A.	– / –
AMD Ryzen Threadripper	✓ / Betriebssystem	✓ / Betriebssyst. u. MCU[1]	– (nur Meltdown-BR) / k. A.	– / –
Intel Core i-8000 (Desktop)	✓ / Betriebssystem	✓ / Betriebssyst. u. MCU[1]	✓ / Betriebssystem	✓ / Betriebssystem
Intel Core i-8000U	✓ / Betriebssystem	✓ / Betriebssyst. u. MCU[1]	✓ / Betriebssystem	✓ / Betriebssystem
Intel Core i-8000U Whiskey Lake	✓ / Betriebssystem	✓ / Betriebssyst. u. MCU[1]	– / –	– / –
Intel Core i-9000 (Desktop)	✓ / Betriebssystem	✓ / Betriebssyst. u. MCU[1]	– / –	– / –

[1] MCU = Microcode Update ✓ vorhanden – nicht vorhanden

Intel, wo bereits verteilte Microcode-Updates nach schweren Fehler auf wenigen Systemen wieder zurückgezogen wurden. Das sorgte für große Verwirrung.

Auch das Ausspielen von Microcode-Updates für Prozessoren via Windows Update, was es in älteren Windows-Versionen schon einmal gab, musste erst wieder neu implementiert werden. Die aktuellen Microcode-Updates für Intel-CPUs kommen 18 Monate nach Bekanntwerden der Probleme noch immer nicht automatisch auf Windows-10-Systeme.

Diese Pannen zeigen, dass die CPU-Hersteller entgegen aller Beteuerungen nicht gut auf große Update-Manöver vorbereitet sind. Die Standard-Firmware für x86-PCs, das UEFI-BIOS, ist zwar mit Funktionen geradezu überfrachtet. An eine einheitliche, sichere, robuste und verpflichtend eingebaute Update-Funktion für Notfälle hat aber niemand gedacht.

AMD und Intel sind aber nicht die einzigen Hersteller, die Kunden im Regen stehen lassen. Google etwa hatte in Bezug auf Android behauptet, mit dem Security Patch Level Januar 2018 das Problem gelöst zu haben. Dabei wurde bloß die Genauigkeit eine Timer-Funktion gedrosselt, um Angriffe via Browser und Spectre zu erschweren. Dass viele Android-Smartphones das Update gar nicht erst bekommen haben, schert Google nicht.

Mittlerweile sind zwar Backports der Linux-Kernel-Patches gegen Spectre und Meltdown in Android eingeflossen – aber man bekommt auf einem individuellen Smartphone kaum heraus, ob diese Patches vorhanden sind. Die CPU-Schmiede ARM hat zwar viele Informationen dazu veröffentlicht, aber bei Chipherstellern wie Qualcomm und Samsung und erst recht bei Smartphone-Herstellern versandet der Informationsfluss: Es interessiert sie einfach nicht.

CPU-Sicherheitslücken Spectre(-NG) und Meltdown

(Google-)Name	Bezeichnung	weitere Bezeichnung	CVE-Nummer
Spectre V1	Bounds Check Bypass (BCB)	Spectre-PHT	CVE-2017-5753
Spectre V1.2	Read-only Protection Bypass	Meltdown-RW	k. A.
Spectre V2	Branch Target Injection (BTI)	Spectre-BTB	CVE-2017-5715
Meltdown = Spectre V3	Rogue Data Cache Load	Meltdown-US	CVE-2017-5754
Spectre-NG			
Spectre V1.1	Bounds Check Bypass Store (BCBS)	Spectre-PHT	CVE-2018-3693
Spectre V3a	Rogue System Register Read (RSRE)	Meltdown-GP	CVE-2018-3640
Spectre V4	Speculative Store Bypass (SSB)	Spectre-STL	CVE-2018-3639
k. A.	Lazy FP State Restore	k. A.	CVE-2018-3665
Foreshadow	L1 Terminal Fault (L1TF) – SGX	k. A.	CVE-2018-3615
k. A.	L1 Terminal Fault (L1TF) – OS, SMM	k. A.	CVE-2018-3620
k. A.	L1 Terminal Fault (L1TF) – VM	k. A.	CVE-2018-3646
Spectre-Varianten via Return Stack Buffer (RSB)			
„Spectre V5“	ret2spec	k. A.	k. A.
k. A.	SpectreRSB	Spectre-RSB	CVE-2018-15572
sonstige Spectre- und Meltdown-Varianten			
k. A.	BranchScope	k. A.	CVE-2018-9056
k. A.	SGXPectre, NetSpectre (nutzen V1)	k. A.	k. A.
k. A.	Meltdown-NM	FPU Register Bypass	k. A.
k. A.	Meltdown-P	Virtual Translation Bypass	k. A.
k. A.	Meltdown-BR (ähnelt Spectre-PHT)	Bounds Check Bypass	k. A.
k. A.	Meltdown-PK	Protection Key Bypass, MPX	k. A.

k. A. keine Angabe

Neue Konzepte

Prozessorentwickler und Sicherheitsexperten haben 2018 auf mehreren internationalen Konferenzen über Schutzfunktionen für sicherere Prozessoren diskutiert. Bis solche Konzepte jedoch in tatsächlich kaufbare Prozessoren für Notebooks und Desktop-PCs eingeflossen sind, werden noch Jahre ins Land gehen.

Die 2019 von AMD und Intel erwarteten neuen Prozessoren sind nicht grundsätzlich frei von Spectre-Lücken, aber nicht mehr durch Meltdown und L1TF angreifbar. Vor den verbleibenden Spectre-Risiken schützen Updates der Betriebssysteme.

Nutzer im Regen

Als Schutz vor potenziellen Angriffen durch Spectre und Meltdown kann man weiterhin nur ständige Updates empfehlen, vor allem des Betriebssystems. Aber auch nach BIOS-Updates sollte man immer mal wieder schauen. Diese schließen ja auch Lücken im UEFI-BIOS, von denen in den vergangenen Monaten auch einige aufgedeckt wurden.

Um es abermals zu betonen: Es gibt keinen Grund zur Panik wegen Spectre und Meltdown. Trotzdem ist das Verhalten von AMD und Intel sehr ärgerlich. Man wünscht sich mehr und klarere Informationen sowie schnellere Reaktionen. Es entsteht der Eindruck, dass die CPU-Hersteller lieber ihre Aktionäre schützen als ihre Kunden. Die zahlreichen Pannen beweisen zudem wieder einmal, dass die IT-Industrie mit der Sicherheit auf Kriegsfuß steht: Auf dem Weg vom Programmierer bis zum Endnutzer muss ein Sicherheitspatch zu viele Hürden überwinden. Das verlängert nicht nur die Zeit, bis ein System geschützt werden kann, sondern trägt auch dazu bei, dass viele Rechner überhaupt keine Patches bekommen.

Nun sind Spectre und Meltdown zwar tief gehende Sicherheitslücken, aber auch nur einige unter tausenden – und je nach Betriebssystem und konkreter Gefährdung des Rechners auch nicht die schwerwiegendsten. Am Ende helfen eben nur ständige Updates – notfalls sogar der Hardware. *(ciw@ct.de)* c't

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover