Riesenlücken weiter offen

Patch-Chaos bei Meltdown und Spectre

Die Anfang Januar veröffentlichten Sicherheitslücken in Prozessoren von Intel, AMD und vielen anderen Herstellern sind erst auf wenigen Systemen geschlossen. Vor allem BIOS-Updates machen Probleme.

Von Christof Windeck

Die Hiobsbotschaften reißen nicht ab: Statt zügig weiter BIOS-Updates bereitzustellen, zogen Intel, einige PC-Hersteller sowie Linux-Distributoren und VMware einige der bereits ausgelieferten Updates wieder zurück. Das vergrößert die Unsicherheit weiter und lässt Millionen von Rechnern ohne vollständigen Schutz vor allem vor der Sicherheitslücke Spectre Variante 2 alias Branch Target Injection (BTI, CVE-2017-5715) zurück.

Was bisher geschah

Wie in c't 3/2018 berichtet, haben Experten unter anderem von Google und von der TU Graz schon im Juni 2017 die drei Sicherheitslücken Meltdown, Spectre Variante 1 und Spectre Variante 2 entdeckt. Sie nutzen Funktionen, die in allen aktuellen PC- und Server-Prozessoren und sehr vielen ARM-SoCs für Smartphones stecken. Daher informierten die Entdecker zunächst nur die CPU-Hersteller AMD und Intel sowie den CPU-Entwickler ARM. Man vereinbarte, bis zum 9. Januar 2018 Updates bereitzustellen und zu diesem Zeitpunkt die Öffentlichkeit zu informieren. Doch die Lücke wurde bereits am 3. Januar bekannt.

Trotz sechs Monaten Vorlauf ist es nicht gelungen, alle Lücken vollständig zu schließen. Geklappt hat es nur für Meltdown – davon sind nur Intel-Prozessoren betroffen –, und zwar durch Updates für 64-Bit-Betriebssysteme (Windows, Linux, macOS 10.13). Microsoft hat Updates für 32-Bit-Windows nachgereicht, für Linux sind welche in Arbeit. Apple stellt Updates nun auch für die älteren macOS-Versionen 10.11 (El Capitan) und 10.12 (Sierra) bereit.

Die Spectre-Variante 1 gilt unter Windows und macOS als weitgehend geschlossen. Der Linux-Kernel soll mit Version 4.16 Gegenmaßnahmen bekommen (siehe S. 32), einige Distributionen haben sie bereits in ihre Kernel eingebaut. Die meisten Probleme gibt es derzeit bei Patches für Spectre Variante 2, also BTI. Glück im Unglück: Laut den Experten von der TU Graz ist es für Malware-Programmierer schwierig, BTI zu nutzen. Bisher sind auch keine Exploits im Umlauf, also kein Schadcode, der BTI nutzt. Und laut AMD konnte BTI auf AMD-Prozessoren noch nicht demonstriert werden.

Die Probleme

Um die BTI-Lücken zu stopfen, gibt es mehrere Ansätze, was den Überblick erschwert. Die Linux-Kernel-Entwickler haben sich für den von Google entwickelten Schutz namens Retpoline entschieden, der auf den meisten Prozessoren ohne weitere Updates funktioniert. Einige Linux-Distributionen wie RHEL und SLES sowie Microsoft bei Windows setzen hingegen auf Indirect Branch Control (IBC), die wiederum neue CPU-Funktionen namens IBPB, IBRS und STIBP benötigt. Letztere wollen AMD und Intel mit CPU-Microcode-Updates nachrüsten, doch hier klemmt es derzeit gewaltig.

Die bis Mitte Januar bereits zum Download bereitgestellten BIOS-Updates für Intel-Systeme mit den erwähnten Microcode-Updates verursachten bei mehreren Core-i-Generationen und den damit verwandten Xeons Probleme wie spontane Neustarts. Deshalb hat Intel diese Updates am 22. Januar wieder zurückgezogen. Damit ist nun völlig unklar, zu welchem Zeitpunkt für welche Computer Microcode- beziehungsweise BIOS-Updates bereitstehen – erst nach Redak-

Table 2-2. CPUID Leaf 07H, Sub-leaf 0: Updated EDX Register Details

Initial EAX Value		Information Provided About the Processor
Structured Extended Feature Flags Enumeration Leaf (Output depends on ECX input value)		
07H		**NOTES:** Leaf 07H main leaf (ECX = 0). If ECX contains an invalid sub-leaf index, EAX/EBX/ECX/EDX return 0.
	EDX	Bits 25-00: Reserved Bit 26: IBRS and IBPB supported Bit 27: STIBP supported Bit 28: Reserved Bit 29: IA32_ARCH_CAPABILITIES supported Bits 31-30: Reserved

Intel dokumentiert nun die neuen Prozessorfunktionen zum Schutz gegen Branch Target Injection (BTI).

tionsschluss dieser c't-Ausgabe will Intel weitere Informationen liefern.

Für Systeme, die wegen der Microcode-Updates spontan neustarten, hat Microsoft das optionale Windows-Update KB4078130 bereitgestellt, welches den Spectre-Schutz deaktivieren kann; das ist allerdings per Registry-Eingriff möglich.

AMD sieht die eigenen Prozessoren zwar nicht im gleichen Ausmaß durch BTI gefährdet wie Intel-Chips, will aber trotzdem ebenfalls Microcode-Updates liefern. Doch AMD verrät nicht, wann und für welche Prozessoren außer den aktuellen Ryzen und Epyc diese Updates kommen werden. Auch Intel verweigert bislang Angaben zu älteren Prozessoren außer Core i-4000 (Haswell), Core i-5000 (Broadwell), Core i-6000 (Skylake), Core i-7000 (Kaby Lake) und Core i-8000 (Coffee Lake).

Windows-Rechner mit Windows-Updates, aber ohne BIOS-Update, sind nicht vor BTI geschützt. Experten raten zu Schutzmaßnahmen wie Skriptblockern für Browser (siehe S. 156) und Zwei-Faktor-Authentifizierung; Firmen können den Zugang auf ihre Systeme auch auf bestimmte IP-Bereiche eingrenzen, um Risiken zu mindern.

Bei manchen Linux-Distributionen und beim Hypervisor VMware ESXi sind keine BIOS-Updates nötig; hier kommen Microcode-Updates über Updates der jeweiligen Distribution aufs System. Doch auch diese Updates wurden zurückgezogen, was vor allem Rechenzentren vor Probleme stellt. Linus Torvalds äußerte mehrfach harsche Kritik an Intels Vorgehen sowie am Patch-Code.

Der Compiler GCC 7.3 bringt neue Schalter für Schutz gegen Spectre V2 mit. Microsoft hat in den C/C++-Compiler von Visual Studio 2017 Version 15.5 die Option /d2guardspecload als Schutz vor Spectre V1 integriert.

Bei Smartphones und Tablets mit iOS und Android hat sich die Situation in den vergangenen zwei Wochen seit unseren Berichten in c't 3/2018 nicht verändert: Neue Android-Versionen kommen mit Patches, zu älteren Smartphones äußern sich die meisten Hersteller bisher nicht. Samsung vertröstet etwa im Supportforum Käufer des aktuell noch angebotenen Galaxy Tab S2 mit Android 6 und Snapdragon 652 (Cortex-A72). Apple schließt die Lücken mit iOS 11.2 und weiteren Updates, lässt aber ältere iOS-Versionen ungeschützt, also ältere iPads und iPhones bis zum iPhone 5(C).

Sichere Prozessoren

Anlässlich der Verkündung der (übrigens sehr guten) Geschäftszahlen 2017 kündigte Intel-CEO Brian Krzanich noch für 2018 erste Prozessoren mit verbesserter Hardware an. Welche das sind, wann sie kommen und welche Lücken sie schließen, ließ er aber offen. Denkbar wäre außer den erwähnten IBC-Funktionen als Schutz vor BTI auch die bereits 2016 angekündigte Control-flow Enforcement Technology (CET), die Krzanich aber nicht erwähnt.

Es gibt ARM-Prozessoren mit Rechenkernen wie Cortex-A7 und Cortex-A53, die nicht von Spectre betroffen sind, etwa der BCM2837 des Raspberry Pi 3. Der Raspi 3 läuft unter Linux, ist aber nur für wenige Anwender eine Alternative zu einem normalen PC oder Notebook. Android-Geräte mit nicht betroffenen Cortex-Kernen sind nur dann sicher, wenn sie ausreichend häufig Android-Updates erhalten, die andere Sicherheitslücken schließen. Doch bekanntlich liefern die meisten Hersteller von Android-Smartphones und -Tablets recht selten Updates.

Wer prüfen will, ob sein Windows-PC alle Updates gegen Meltdown und Spectre aktiviert hat, kann dazu das in c't 3/2018 ab Seite 66 vorgestellte PowerShell-Skript SpeculationControl von Microsoft nutzen. Obwohl es etwas kompliziert zu bedienen ist, raten wir von anderen Tools ab: Mangels genauer Dokumentation sind deren Angaben weniger verlässlich und es besteht obendrein die Gefahr, dass Trittbrettfahrer vermeintliche Prüf-Software nutzen, um etwa Trojaner einzuschleusen.

Chaos bleibt

Die Gefahr in Bezug auf Meltdown scheint im Wesentlichen gebannt. Doch bei den Spectre-Lücken, vor allem bei der zweiten Variante BTI, herrscht das blanke Chaos. Noch immer fehlen genaue Informationen. Das betrifft auch Server und Embedded Systems: So sind etwa auch einige IBM-Power-Prozessoren betroffen, die MIPS-Kerne P5600 und P6600 sowie kommende ARM64-Server-SoCs wie Qualcomm Centriq 2400 und Cavium ThunderX2.

Allerdings sollte man die Gefahr durch BTI nicht überbewerten: In Betriebssystemen, BIOSsen, Browsern und Anwendungssoftware werden ständig neue Lücken entdeckt, die Updates manchmal erst nach Wochen oder Monaten schließen. Darunter sind immer wieder kritische Angriffsmöglichkeiten, manche zudem leichter nutzbar als BTI. So gesehen ist BTI ein Risiko unter vielen. Man sollte Updates aber zügig einspielen, sichere sowie unterschiedliche Passwörter für verschiedene Online-Dienste wählen und möglichst Multi-Faktor-Authentifizierung nutzen. Skriptblocker verstärken den Schutz. Vor allem aber ist es wichtig, Risiken zu meiden, etwa zweifelhafte Webseiten und Software aus dubiosen Quellen. *(ciw@ct.de)* c't

Die CPU-Sicherheitslücken Meltdown und Spectre

Google-Name	Kurzbezeichnung	CVE-Nummer
Spectre, Variante 1	Bounds Check Bypass	CVE-2017-5753
Spectre, Variante 2	Branch Target Injection (BTI)	CVE-2017-5715
Meltdown	Rogue Data Cache Load	CVE-2017-5754