Spectre-NG-Lücke Nummer 3

Am 13. Juni hat Intel mit dem Sicherheitshinweis SA-00145 Informationen zu einer Sicherheitslücke namens Lazy FP State Restore veröffentlicht. Sie wird mit der CVE-Nummer CVE-2018-3665 geführt und ist die dritte der insgesamt acht neuen „Spectre NG“-Sicherheitslücken, über die c’t Anfang Mai berichtet hat. Die Veröffentlichung erfolgte anders als geplant nicht in einem koordinierten Verfahren, weil Details überraschend schon früher bekannt wurden: Auf einer Konferenz zu BSD-Betriebssystemen hatte OpenBSD-Gründer Theo de Raadt am 9. Juni Informationen präsentiert. Der für deutliche Worte bekannte de Raadt sparte dabei nicht mit Kritik an Intel.

Entdeckt wurden die Sicherheitsrisiken im Zusammenhang mit der Technik Lazy FP State Restore von Amazon und der deutschen Firma Cyberus Technology. Ihnen war aufgefallen, dass auch Daten, die in den Registern der Gleitkomma-Rechenwerke (Floating Point Units, FPU) von Intel-Prozessoren stehen, unter bestimmten Bedingungen über Seitenkanäle von einem dazu nicht berechtigten Prozess gelesen werden können. In diesen FP-Registern stehen Werte, welche die AVX-, SSE- und MMX-Einheiten der CPU verarbeiten. Diese Einheiten verwenden auch die AES New Instructions (AES-NI), um Krypto-Algorithmen zu beschleunigen. Daher lassen sich über den Missbrauch von Lazy FP State Restore möglicherweise geheime Schlüssel ablauschen.

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 (GPZ V3)	Rogue Data Cache Load	CVE-2017-5754
Spectre Variante 3a	Rogue System Register Read (RSRE)	CVE-2018-3640
Spectre Variante 4	Speculative Store Bypass (SSB)	CVE-2018-3639
k. A.	Lazy FP State Restore	CVE-2018-3665

Zu fünf weiteren Spectre-NG-Lücken fehlen noch Informationen.
GPZ steht für Google Project Zero, Spectre V1 und V2 werden auch GPZ V1 und GPZ V2 genannt.

Abhilfe ist relativ einfach: Statt Lazy FP State Restore müssen das Betriebssystem beziehungsweise Systemprogramme Eager FP State Restore verwenden. Dann sind die Daten in den FP-Registern bei Task-Wechseln besser geschützt. Als Patches sind daher diesmal keine CPU-Microcode-Updates oder Firmware-Updates nötig, sondern nur Updates für Betriebssysteme. Daher waren eben auch OpenBSD-Entwickler informiert, ebenso wie Linux-Kernel-Entwickler. Unter ct.de/y1gz sammeln wir Links zu den Info- und Update-Seiten von Herstellern betroffener Produkte.

Microsoft scheint von der frühen Veröffentlichung der neuen Sicherheitslücke überrascht worden zu sein. Bis zum Redaktionsschluss vertröstete das Advisory ADV180016 auf später.

(ciw@ct.de)

Literatur

[1] Jürgen Schmidt, Wieder verspekuliert, Super-GAU für Intel: Weitere Spectre-Lücken im Anflug, c’t 11/2018, S. 16

Hersteller-Informationen zu Spectre-NG: ct.de/y1gz

Anzeige

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