Spectre-Stopfen

Erste Updates gegen die Sicherheitslücken „Spectre NG“

Unter der Bezeichnung Spectre Next Generation hatte c’t Anfang Mai acht neue Sicherheitslücken in Prozessoren von Intel, ARM, AMD und IBM dokumentiert. Für Spectre V3a und Spectre V4 kommen nun Updates und Informationen.

Von Christof Windeck

Am 21. Mai rückten AMD, ARM, IBM und Intel mit Update-Plänen und technischen Details zu den Sicherheitslücken Spectre V3A und Spectre V4 heraus. Sie stimmen mit den c’t vorab vorliegenden Informationen weitgehend überein. Details zu sechs weiteren Spectre-NG-Sicherheitslücken werden erst in den kommenden Monaten erwartet.

Die Informationen zu Spectre V3A alias Rogue System Register Read (RSRE) und Spectre V4 (Speculative Store Bypass, SSB) wurden in einer koordinierten Veröffentlichung bekannt gegeben. Beide Sicherheitslücken sind Seitenkanalattacken, die ähnlich wie Spectre funktionieren, und sind als „mittlere“ Sicherheitsrisiken eingestuft. Weiterhin sind keine praktischen Angriffe über Spectre-Lücken bekannt. Bei typisch genutzten Desktop-PCs und Notebooks stellen sie ein vergleichsweise geringes zusätzliches Risiko dar, weil dort üblicherweise mehrere andere, leichter nutzbare Sicherheitslücken klaffen. Intel betont zudem, dass sich Spectre V3A nach derzeitigem Wissensstand bei Intel-Prozessoren kaum praktisch nutzen lässt.

Updates

Laut Intel sind die wichtigsten Schutzmaßnahmen gegen Spectre V3A und V4 für PCs bereits umgesetzt oder in der Umsetzung begriffen: Seit Januar erscheinen Updates für Webbrowser, die es Schadsoftware noch schwerer machen, Spectre-Lücken zu nutzen. Dazu gehört „Timer Fuzzing“: Bestimmte Timer-Funktionen in JavaScript arbeiten nun weniger genau. Für die Angriffe ist es nämlich wichtig, die für das Ausführen bestimmter Befehle benötigte Zeit exakt zu messen. Erst in der Betaphase ist „Site Isolation“: Browser führen bestimmte JavaScript-Programme in voneinander getrennten Prozessen aus. Auch für Linux gibt es bereits Patches.

Im Laufe der kommenden Monate will Intel jedoch auch neue CPU-Microcode-Updates für praktisch alle Prozessoren seit 2011 verteilen, so wie es als Schutz gegen Spectre V2 geschieht. Für viele Prozessoren kommen sie per Windows Update automatisch, zumindest bei Windows 10. Aber es wird auch BIOS-Updates geben. Die Microcode-Updates bringen den Prozessoren neue Features bei, die nicht automatisch aktiv sind. Betriebssysteme und Software können sie nutzen, um den Schutz in kritischen Code-Abschnitten oder allgemein zu verstärken. Vor Spectre V4 soll die Möglichkeit schützen, die Funktion Memory Disambiguation (MD) abzuschalten. Das geht aber mit einem Verlust an Rechenleistung einher, den Intel auf 2 bis 8 Prozent beziffert.

AMD spendiert künftigen Prozessoren ein zusätzliches Bit im Machine-Specific Register (MSR) 48h, um SSB abzuschalten. In einem Whitepaper erklärt AMD, wie sich SSB bei bisherigen Prozessoren abschalten lässt.

Zum Schutz gegen Spectre V3A bringt Intel ebenfalls Microcode-Updates, die es Programmierern ermöglichen, das Auslesen bestimmter Prozessor-Register feiner zu steuern. Laut AMD sind die hauseigenen Prozessoren nicht von Spectre V3A betroffen. Unter ct.de/yb4c sammeln wir Links zu Info- und Update-Seiten.

(ciw@ct.de) c't

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/yb4c***

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

zu sechs 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