GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

GWDG-Sicht auf Spectre und Meltdown

Die Sicherheitslücken **CVE-2017-5753**[1] (Spectre 1, Bounds Check Bypass), **CVE-2017-5715**[2] (Spectre 2, Branch Target Injection) und **CVE-2017-5754**[3] (Spectre 3 oder Meltdown, Rogue Data Cache Load) wurden Ende 2017 öffentlich bekannt. Insbesondere die Spectre-Lücken Variante 1 und 2 betreffen praktisch alle modernen Prozessoren sämtlicher Hersteller. Gemeinsam haben alle Lücken, dass ein im User Space laufender Prozess Lesezugang zu Speicherbereichen anderer Prozesse oder Lesezugang zum Kernel-Speicher erlangen kann. Bei einem erfolgreichen Angriff sind alle Geheimnisse (Passwörter, Credentials, allg. Daten) in Gefahr, abgegriffen zu werden. Auf Einzelplatzsystemen besteht im Wesentlichen durch Angriffe via Javascript Gefahr. Hierzu können und sollten natürlich die bereits zur Verfügung gestellten Browser-Updates eingespielt werden. Insbesondere auf Systemen mit mehreren Benutzern (Login-Systeme, der High-Performance-Computing-Bereich [HPC], Cloud Server) besteht aber Handlungsbedarf. Im Falle eines Cloud Servers besteht sogar die Gefahr, dass eine virtuelle Maschine den Speicher anderer Maschinen auf demselben Host ausliest.

Spectre Variante 1 ist mit einem Kernel-Update ohne nennenswerte Performance-Probleme einfach zu schließen. Spectre Variante 3 (Meltdown) betrifft nur Intel- (und einige ARM-)CPUs und ist mit Performance-Einbußen durch ein Kernel-Update zu schließen. Wir empfehlen, die Patches gegen Meltdown (und Spectre Variante 1) in jedem Fall einzuspielen, da Meltdown vergleichsweise leicht ausgenutzt werden kann und mit wenig Aufwand der vollständige Speicher eines Rechners (inkl. aller virtuellen Maschinen im Falle von Cloud Servern) ausgelesen werden kann.

Im Folgenden geht es um die Probleme und Ansätze bezüglich Spectre Variante 2. Diese Lücke ist nicht so einfach zu beheben und kann deutliche Leistungsprobleme nach sich ziehen.

Ansatz 1: Neue CPU-Funktionen (IBRS/IBPB) müssen durch Microcode-Update nachgerüstet werden. Gleichzeitig müssen diese Funktionen vom Kernel verwendet werden, um Prozesse und Kernel gegeneinander abzusichern. Ebenso müssen Hypervisor einer Virtualisierungsschicht diese Funktionen verwenden, um virtuelle Maschinen gegeneinander abzusichern.

Ansatz 2: Eine neue Compiler-Funktion „Retpoline“ (return trampoline) sorgt auf Compiler-Ebene dafür, dass der erzeugte Code keine angreifbare spekulative Ausführung mehr beinhaltet. Bei diesem Ansatz muss der Kernel mit Retpoline kompiliert sein, und *jede Software*, die zu schützende Geheimnisse enthält, muss ebenso mit Retpoline neu übersetzt werden.

Hier muss man Vor- und Nachteile abwägen. Insbesondere Ansatz 1 führt nach unseren Messungen im HPC-Bereich zu erheblichen, inakzeptablen Leistungseinbußen und funktioniert nur auf CPUs deren Microcode-Update freigegeben wurde. Ansatz 2 beinhaltet das Neuübersetzen zumindest aller „systemkritischen“ Programme, führt aber zu weniger oder keinem[4] Leistungseinbruch. Die verschiedenen Distributoren setzen zur Zeit auf unterschiedliche Ansätze zur Behebung.

Unserer Einschätzung nach sollte man bei dieser Lücke nicht zu voreilig verfahren. Jedes System muss auf die Art der Verwendung hin geprüft werden und ob dabei tatsächlich eine wahrscheinliche Gefahr des Speicherauslesens besteht. Bis auf die durch Browser-Updates bereits verhinderten Angriffe via Javascript gibt es bislang nur einfache, stark beschränkte Proof-of-Concept-Angriffe auf Spectre Variante 1 und 2, sodass bislang noch kein echter Schädling für diesen Angriff bekannt ist. Für Systeme mit mehreren Nutzern ist das Absichern langfristig sicherlich nötig. Bis dahin wird sich aber ein favorisierter Weg aller Distributoren durchsetzen, der vermutlich durch Retpoline kritische Software wie Kernel, PAM, LDAP, Browser oder ähnliches speziell schützt. Zumindest die Entwicklung des offiziellen Linux-Kernels deutet auf diesen Weg hin. Bei Microsoft scheint sich der Ansatz 1 durchzusetzen.

---

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754
[4] https://www.theinquirer.net/inquirer/news/3024392/google-claims-its-spectre-patch-results-in-no-degradation-to-system-performance