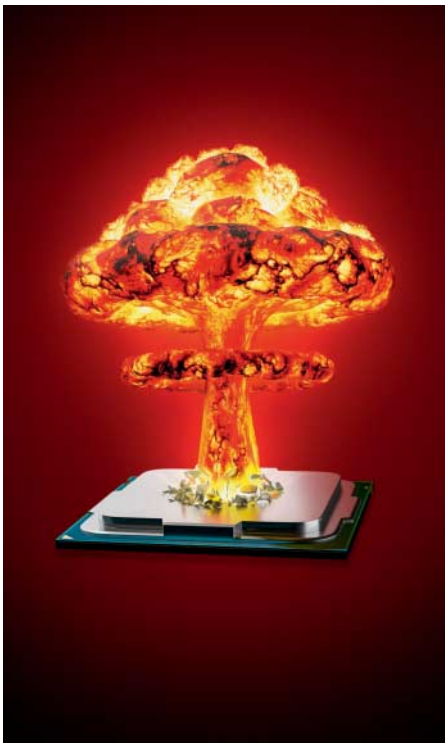
Zombie-Daten

Neue Sicherheitslücke „ZombieLoad“ in Intel-Prozessoren



Nach Spectre und Meltdown decken Experten nun weitere Schwachstellen in Intel-Prozessoren auf, über die Malware Daten ausspähen kann. Nur die jüngsten CPUs sind geschützt.

Von Christof Windeck

Die Bugs nehmen kein Ende: Auch die ZombieLoad getaufte Sicherheitslücke in Intel-Prozessoren erlaubt es bösartiger Software, vermeintlich geschützte Daten eines parallel laufenden Programms zu lesen. Das klappt sogar, wenn die Schadsoftware in einer anderen virtuellen Maschine läuft als das Software-Opfer. Voraussetzung ist allerdings, dass Aggressor- und Opferprozesse auf demselben physischen Prozessorkern laufen. Besonders gut funktioniert ZombieLoad, wenn Hyper-Threading (HT) aktiv ist, weil sich die Prozesse dann mehr Ressourcen teilen.

Betroffen von ZombieLoad sind Intel-Prozessoren aller Core-i- und Xeon-Generationen ungefähr seit dem Jahr 2011. Erst bei den neuesten Varianten der neunten Core-i-Generation (Core i3-/i5-/i7-/i9-9000 alias Coffee Lake Refresh) hat Intel einen Hardware-Schutz eingebaut. Die ersten ausgelieferten Versionen des Core i9-9900K (Stepping 12) kamen jedoch noch ohne. Geschützt sind auch die Whiskey-Lake-Mobilprozessoren, also bestimmte Versionen der Baureihe Core i-8000U, sowie die Xeon-SP-Typen der zweiten Generation Cascade Lake.

Für ältere Prozessoren stellt Intel Microcode-Updates bereit, die zusammen mit Patches für Betriebssysteme und Hypervisoren gegen ZombieLoad schützen sollen. Lassen sich solche Patches nicht einspielen, empfehlen die Entdecker von ZombieLoad, Hyper-Threading (HT) abzuschalten. Doch selbst dann funktionieren Teile von ZombieLoad noch.

Risiko „mittel“

ZombieLoad bedroht vor allem Nutzer und Betreiber von Cloud-Rechenzentren, auf deren Servern virtuelle Maschinen (VMs) unterschiedlicher Kunden laufen. Hier kann ein Angreifer leicht eine VM mit bösartigem Code starten. Bei PCs, Notebooks und Tablets – sogenannten Client-Systemen – hängt die Bedrohungslage von mehreren Faktoren ab. Auf vielen Windows-PCs etwa gibt es andere Sicherheitslücken, die sich leichter für Attacken missbrauchen lassen. Folglich dürfte ZombieLoad nicht die erste Wahl als Angriffsmethode sein – es sei denn, es geht um einen gezielten (Spearhead-) Angriff auf ein besonders wichtiges System. Ähnliches gilt für hochsicher konfigurierte Linux-Rechner, auf denen man sensible Daten bearbeitet.

Intel hat noch drei verwandte Sicherheitslücken aufgedeckt und spricht zusammenfassend von Microarchitectural Data Sampling (MDS). Damit lassen sich Daten nicht verändern, sondern nur lesen; außerdem kann der Angreifer höchstens indirekt beeinflussen, welche Daten – also von welchen Speicheradressen – gelesen werden sollen. Der Angriff muss deshalb entweder genau zum richtigen Zeitpunkt oder sehr lange laufen, um sensible Daten „mitzuschneiden“.

An der Entdeckung von ZombieLoad war jenes Team der TU Graz beteiligt, das auch schon an Spectre und Meltdown mitarbeitete. Auch die Firma Cyberus Technology trug zur Aufdeckung beider Lücken bei und hat ein Video veröffentlicht, welches einen ZombieLoad-Angriff unter dem als besonders sicher geltenden Linux Tails demonstriert, siehe ct.de/y3sz. Dabei liest eine parallel laufenden Software Daten des Tor-Browsers mit, obwohl der in einer virtuellen (qemu-)Maschine läuft. Die weiteren MDS-Schwachstellen Fallout, Yet another Meltdown Attack (YAM) und RIDL wurden unter anderem von der Firma Bitdefender und der Uni Amsterdam beigesteuert.

Updates

Die Veröffentlichung der MDS-Lücken erfolgte koordiniert am Microsoft-Patchday 14. Mai. Für aktuelle Windows-Versionen gibt es bereits Updates, ebenso wie für viele Linux-Distributionen, den Linux-Kernel, für FreeBSD sowie für Hypervisoren wie Xen und VMware ESXi. Apple hat eine Anleitung veröffentlicht, wie man macOS-Systeme schützt. Verweise zu Updates, zu Demo-Videos und zu genaueren Erklärungen für Experten finden Sie auf ct.de und über ct.de/y3sz.

(ciw@ct.de) c't

ZombieLoad-Updates: **ct.de/y3sz**

MDS-Sicherheitslücken in Intel-Prozessoren

Sicherheitslücke	CVE-Nummer
Microarchitectural Store Buffer Data Sampling (MSBDS), Fallout	CVE-2018-12126
Microarchitectural Fill Buffer Data Sampling (MFBDS), ZombieLoad, RIDL, YAM	CVE-2018-12130
Microarchitectural Load Port Data Sampling (MLPDS)	CVE-2018-12127
Microarchitectural Data Sampling Uncacheable Memory (MDSUM)	CVE-2019-11091