



Bitdefender entdeckt neue Schwachstelle in Intel Prozessoren - Detailwissen zur Schwachstelle würde Angreifern weltweit die Möglichkeit zu Datendiebstahl, Erpressung, Spionage und Sabotage eröffnen

Bitdefender hat eine neue Sicherheitslücke identifiziert, die sämtliche moderne Intel Prozessoren betrifft. Diese Prozessoren nutzen die CPU-Funktion Speculative Execution, über die eine Side-Channel-Angriffe erfolgen kann. Die Schwachstelle ermöglicht Zugriff auf Passwörter, Token, private Unterhaltungen sowie andere vertrauliche Daten von Privatanwendern und Unternehmen. Alle Rechner, bei denen neuere Intel-Prozessoren zum Einsatz kommen und auf denen Windows ausgeführt wird, sind betroffen, inklusive Server und Notebooks. Über ein Jahr hat Bitdefender mit den Technologiepartnern an einer Veröffentlichung dieser Schwachstelle gearbeitet. Patches stehen nun zur Verfügung oder werden in Kürze veröffentlicht.

Die Schwachstelle wurde weniger als drei Monate nach dem letzten Sicherheitsalert zu Intel-Prozessoren bekannt. Speculative Execution ist eine Funktion, die darauf abzielt, die Geschwindigkeit der CPU zu beschleunigen, indem Vermutungen darüber getroffen werden, welche Anweisung als nächstes folgen könnte. Speculative Execution kann Spuren im Cache hinterlassen, die es Angreifern ermöglichen, mit einem Seitenkanalangriff in den privilegierten Bereich des Arbeitsspeichers einzudringen, den der Betriebssystem-Kernel belegt. Dieser neu entdeckte Angriffsweg kombiniert Speculative Execution von Intel und die Verwendung eines spezifischen Befehls des Windows Betriebssystems innerhalb eines sogenannten Gadgets.

Der Angriff umgeht alle bekannten Schutzmechanismen, die nach Bekanntwerden von Spectre und Meltdown im Frühjahr 2018 implementiert wurden. Gemeinsam mit Intel hat Bitdefender über ein Jahr daran gearbeitet, nun die Öffentlichkeit über diesen Angriffsmechanismus informieren zu können.

Die Erforschung solcher Angriffswege ist höchst komplex, da sie erstens tiefstes Wissen über die Funktionsweise moderner Prozessoren, zweitens ein umfassendes Verständnis der Prozesse innerhalb von Prozessoren und Betriebssystemen sowie drittens Kenntnisse von Speculative Execution und Seitenkanalattacken erfordern, so Gavin Hill, Vice President, Datacenter and Network Security Products bei Bitdefender. Und zur potentiellen Gefahrenlage: Kriminelle, die über das Wissen um diese Angriffsmöglichkeit verfügen, wären in der Lage, weltweit die wichtigsten und am besten geschützten Daten von Unternehmen und Privatanwendern zu stehlen oder sie für Erpressung, Sabotage und Spionage zu missbrauchen.

Microsoft und andere Partner haben bereits Patches veröffentlicht, beziehungsweise sind dabei diese zu evaluieren und gegebenenfalls zu veröffentlichen. Die von Bitdefender entwickelte Technologie Hypervisor Introspection (HVI) zum Schutz von virtuellen Maschinen erkennt und verhindert diesen neuen Angriff auf ungepatchten Windows-Systemen.

Die neueste Enthüllung folgt der Mitte Mai dieses Jahres bekanntgewordenen Sicherheitsschwachstelle bei Intel-Prozessoren mit dem Namen Micro-Architectural Data Sampling, die es Angreifern erlaubt, auf privilegierte Kernel-Mode-Informationen zuzugreifen, die bis dahin als unerreichbar für die meisten Anwendungen galten. Weitere Informationen zu diesem Angriffsmechanismus finden Sie auf dem Bitdefender Labs Blog.

Ein technisches Whitepaper findet sich hier:

https://businessresources.bitdefender.com/bybypassing-kpti-speculative-behavior-swaps-instruction?utm_campaign=swaps&utm_source=web