Spectre & Meltdown - kurz zusammengefasst

https://blog.godyo.com/meltdown-spectre-kurze-zusammenfassung/

- CVE-2017-5753 - "Variante 1" - Spectre - Bounds Check Bypass
- CVE-2017-5715 - "Variante 2" - Spectre - Branch Target Injection
- CVE-2017-5754 - "Variante 3" - Meltdown - Rogue Data Cache Load

Spectre und Meltdown Varianten in der Übersicht

Durch diese Sicherheitslücken Spectre & Meltdown können Angreifer mittels Schadcode alle Daten auslesen, die der jeweilige Computer im Speicher / Cache verarbeitet. Demzufolge auch Passwörter, firmeninterne Daten, Schlüssel und beliebige Speicherinhalte. Auch Anti-Viren-Programme können dem derzeit nichts entgegensetzen. Soft- & Hardware-Hersteller sind gleichermaßen zum Handeln gezwungen und müssen ihre Firmware, Betriebssysteme oder auch Applikationen zeitnah aktualisieren.

Betroffene Hard- & Software:

Neben Intel, haben auch AMD, ARM und Fujitsu und viele weitere bereits Informationen über die betroffenen Prozessoren veröffentlicht. Neben den genannten Prozessor-Herstellern bleibt auch eine Vielzahl an Herstellern von Software & Peripherie wie Switches, Router etc. nicht verschont. Eine ausführliche Übersicht aller Soft- & Hardware-Hersteller mit Verlinkungen zu den entsprechenden Infoseiten wurde auf Heise veröffentlicht.

"Variante 1" - Spectre - Bounds Check Bypass

Das Angriffsszenario: unzulässiger Zugriff auf Browser, Speicher/Cache

> *„Variante 1 (bounds check bypass)“ könne nur entgegengewirkt werden, indem jede betroffene Anwendung einzeln angepasst wird. Deshalb werden beispielsweise Google Chrome und Firefox […] Updates erhalten.“*
>
> *(Quelle: Google Project Zero)*

"Variante 2" - Spectre - Branch Target Injection

Das Angriffsszenario: unzulässiger Zugriff auf Browser, Speicher/Cache

> *„Variante 2 (branch target injection)“, von der AMD behauptet praktisch nicht betroffen zu sein*

(„near-zero risk“), könne durch Microcode-Updates des CPU-Herstellers oder durch die neue „Retpoline“-Technik entschärft werden. Jene könne dazu in betroffene Betriebssysteme, Hypervisors, Systemprogramme, Bibliotheken und Anwendungen eingebaut werden.“

(Quelle: Google Project Zero)

"Variante 3" - Meltdown - Rogue Data Cache Load

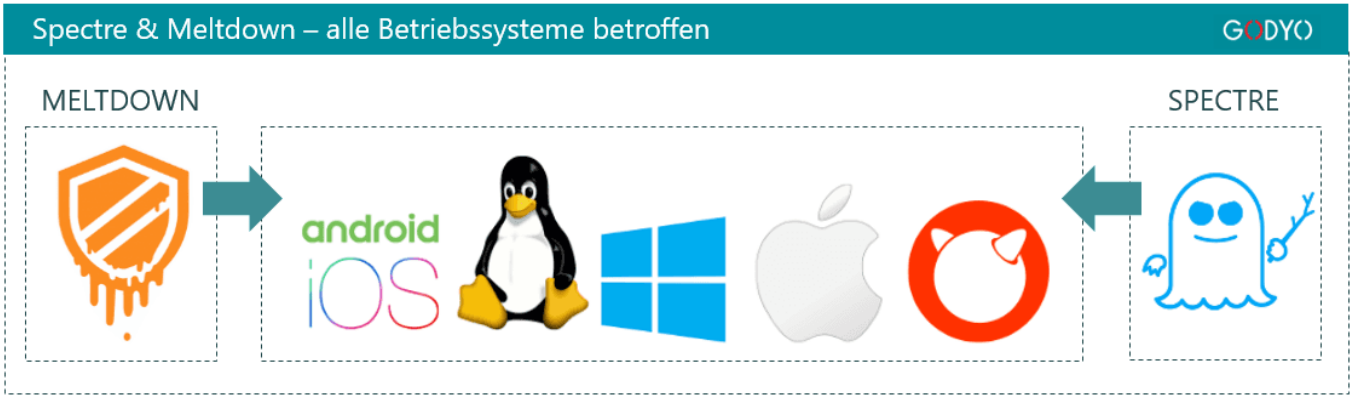
Das Angriffsszenario: Erlangung erweiterter Zugriffsrechte

„Einfach ist der Fall bei Meltdown („Variante 3“): Gegen diese einfach ausnutzbare aber auch relativ einfach behebbare Sicherheitslücke, die ausschließlich Intel-CPUs und wenige ARM-Kerne betrifft, helfen die PTI-Patches für Linux beziehungsweise das heute veröffentlichte Windows-Update.“

(Quelle: Google Project Zero)

Welche Betriebssysteme sind betroffen?

Es sind alle Betriebssysteme betroffen. Von Windows, Linux, Android über MacOS, iOS und FreeBSD.



Spectre und Meltdown - betroffene Betriebssysteme

Was Sie sofort tun können?

Updaten Sie Ihre Browser. Die meisten Browserhersteller haben bereits Updates veröffentlicht oder werden diese in den kommenden Tagen noch veröffentlichen. Google (Chrome-Browser) empfiehlt seinen Nutzern den Punkt Website-Isolierung zu aktivieren. Unter Umständen müssten Sie auch Ihren Systemadministrator beauftragen, die Website-Isolierung (Link für Admins) und Browserupdates global in Ihrem Unternehmen zu veranlassen. Beim Firefox sind ab Version 57.0.4 die entsprechenden Sicherheitsupdates enthalten. Der Patch für Microsofts Browser Edge und Internet Explorer wurde ebenfalls bereits veröffentlich und sollte sich automatisch per Windows-Update installieren.

Ist das Thema nach den Updates erledigt?

Nein. Dafür bedarf es einer neuen Prozessorarchitektur – darauf werden wir aber noch eine Weile warten müssen. Die Updates und Patches verringern aber das Risiko. Einen 100%igen Schutz vor Spectre & Meltdown wird es vorerst nicht geben.

Zum Thema Performance-Einbußen

Es wird wahrscheinlich zu Performance-Einbußen kommen. Teilweise war von über 30% die Rede. Bei hauseigenen Tests kamen wir aber nicht über 10% Performance-Einbußen. Intel veröffentlichte einen Benchmark-Test der dies bestätigt.

Panik und Hysterie bei Spectre & Meltdown!

Derzeit gibt es kein größeres Thema in der IT-Security als Spectre & Meltdown. Beispielsweise sind 90% aller Intel-Prozessoren und etliche Milliarden Soft- & Hardware-Produkte betroffen. Was aber häufig unerwähnt bleibt ist die Tatsache, dass es bisher nur theoretische Angriffsszenarien gibt. Ein realer Angriff ist laut dem BSI noch nicht bekannt geworden.

Daher sollten Sie sensibel mit dem Thema Spectre & Meltdown umgehen, Panik und Hysterie sind in diesem Fall jedoch nicht ratsam und auch nicht erforderlich.

Unsere Spezialisten aus den Bereichen IT-Security und IT-Service helfen täglich Unternehmen die bekannten Sicherheitslücken systematisch zu schließen bzw. Sicherheitsrisiken soweit wie möglich einzudämmen.

Milliarden Geräte sind betroffen, wo anfangen?

Wir empfehlen, dass Sie zuerst alle Geräte updaten oder patchen, die direkt von außen erreichbar sind. Eine kurzzeitige (geräteabhängige) Downtime ist hierbei allerdings unumgänglich. Gemeinsam mit Ihnen stimmen wir etwaige Maßnahmen soweit ab, dass diese möglichst geringe oder keine Ausfallzeiten mit sich bringen.

Update 20. März 2018

VMware hat am Dienstag (20.03.2018) neue Updates für seine Virtualisierungsprodukte – insbesondere VMware vSphere – veröffentlicht, welche aktualisierten Microcode enthalten und damit die so genannten „Hypervisor-Assisted Guest Mitigations“ unterstützen.
https://www.vmware.com/security/advisories/VMSA-2018-0004.html

Intel hat inzwischen für viele seiner Prozessoren so genannte Microcode Updates bereitgestellt (z.B. auch

für die noch weit verbreiteten Xeon E5 v1 Prozessoren - verbaut in HP DL380 G8)
https://newsroom.intel.com/wp-content/uploads/sites/11/2018/03/microcode-update-guidance.pdf

---

Wenn Sie Hilfe dabei benötigen, Ihr System soweit wie möglich zu updaten / patchen, stehen unsere Experten Ihnen mit Rat und Tat zur Seite. Aufgrund der aktuellen Brisanz von Spectre & Meltdown bitten wir Sie, kurze Wartezeiten einzuplanen.

Bei allen Fragen rund um das Thema Spectre & Meltdown wenden Sie sich bitte an:

Ihr Ansprechpartner: Michael Weise

Michael Weise
Leiter Consulting und Solutions
GODYO Enterprise Computing AG
Prüssingstraße 35, 07745 Jena
Telefon: +49 3641 287-0
Telefax: +49 3641 287-287
E-Mail: anfrage@godyo.com
Internet: www.godyo.com