athletec
INDUSTRIE-COMPUTER

Sicherheitslücken Meltdown, Spectre 1 und Spectre 2

Ein Google Forscher-Team konnte letztes Jahr drei gravierende Sicherheitslücken bei Prozessoren ausmachen, die trotz ihrer großen Bedeutung für die Computer-Sicherheit erstaunlich wenig Aufregung bei den Betroffenen ausgelöst haben. Dabei weisen schon die Namen dieser Lücken auf gewaltige Probleme hin, die uns noch jahrelang beschäftigen werden, und für die die Chiphersteller noch keine umfassende Lösung gefunden haben.

Meltdown

„Meltdown" – zu deutsch „Kernschmelze" - betrifft hauptsächlich die Prozessoren von Intel, aber auch die von ARM und Apple. Laut Google haben fast alle Intel-Prozessoren seit 1995 diese Sicherheitslücke, einzig Atom Prozessoren, die bis 2013 hergestellt wurden und Intel Itanium Prozessoren nicht.

Vereinfacht gesagt betrifft die Sicherheitslücke Meltdown die Art und Weise, wie der Prozessor mit Daten umgeht – die Speculative Execution. Diese ermöglicht eine beschleunigte Verarbeitung von Befehlen. Der Prozessor arbeitet die Befehle nicht in der Reihenfolge ihres Eingangs ab, sondern ordnet sie in einem geschützten Speicherbereich neu an. Auf diese Weise können die Befehle möglichst schnell abgearbeitet werden können. Zusätzlich führt der Prozessor Berechnungen durch, um zu kalkulieren, welche Befehle er eventuell noch laden und / oder bearbeiten muss.

Der Bereich, in dem diese Sortierungen und Berechnungen stattfinden, sollte eigentlich gegen Zugriffe von außen geschützt sein - über die Sicherheitslücke Meltdown können Angreifer jedoch Zugriff auf ihn gewinnen und Daten auslesen.

Auf Servern könnten Angreifer über diese Sicherheitslücke unter Umständen an Daten der Nutzer von Online- oder Cloud-Diensten gelangen.

Alle großen Betriebssystemhersteller wie Microsoft, Apple und Linux haben umgehend auf dieses Problem reagiert und Updates ihrer Betriebssysteme bereitgestellt. Die Mitarbeiter der IT sollten dringend überprüfen, ob diese Updates bereits eingespielt wurden. Die Updates lassen sich auch manuell herunterladen.

Außerdem sollten alle Anwendungen, über die sich Schadsoftware einschleusen lässt, wie z.B. Browser oder PDF-Programme, ebenfalls aktualisiert werden. Alle größeren Anbieter solcher Anwendungen haben auf diese Sicherheitslücke ebenfalls reagiert.

Auch die Hersteller von Mainboards bieten BIOS-Updates für Ihre Boards an: Diese Updates sind momentan jedoch nur für die aktuelle Boardgeneration vorgesehen. Wie es mit Updates für ältere Revisionen aussieht, steht noch nicht fest. **Intel rät jedoch mittlerweile von einem BIOS-Update ab.**

gbm Gesellschaft für Bildanalyse und Messwerterfassung mbH • Lehmkuhlenweg 16 • D-41065 Mönchengladbach
Telefon 02161-30899-0 • sales@gbm.de • www.athletec.de

Spectre 1 und Spectre 2

Für die Lücken „Spectre 1“ und „Spectre 2“ – zu deutsch „Schreckgespenst“ - hingegen sind Prozessoren aller Hersteller anfällig, auch jene Prozessoren, die in Smartphones, Tablets, Routern usw. verbaut werden.

Die Spectre Sicherheitslücken ermöglichen es, die Trennung des Speichers einzelner Anwendungen in der CPU zu umgehen. So können Programme, die nur mit eingeschränkten Rechten im User Space des Prozessors laufen, auf Bereiche des Arbeitsspeichers (Kernel Memory) zugreifen, für die sie eigentlich keine Zugriffsberechtigung haben. Dort könnten evtl. Passwörter, Fotos, Mails usw. von Unbefugten ausgelesen werden.

Wie bei der Meltdown-Lücke sollten auch hier die Betriebssystemupdates eingespielt und die Anwendungen aktualisiert werden.

Diese Lücken werden von allen Software- und Hardware-Herstellern als schwerwiegend betrachtet. Die Geschwindigkeit erkennen, mit der Updates für die Betriebssysteme und die Anwendungen bereitgestellt wurden, ist ein Indiz dafür.

Virtuelle Maschinen wie ESXi von VMware oder Microsofts HyperV sind eigentlich sehr gut geschützt gegen Schadsoftware, da sie auf einem isolierten Bereich des Hosts ausgeführt werden. Durch die Sicherheitslücken Spectre 1, Spectre 2 und Meltdown sind nun jedoch ein „Ausbrechen“ des Schadcodes und eine Kompromittierung des Hosts möglich, da diese isolierten Bereiche des Hosts offen stehen.

Microsoft und VMware haben umgehend mit Sicherheitsupdates auf diese Bedrohung reagiert.

Alle Anbieter von Cloud-Lösungen (Amazon AWS, Microsoft usw.) haben nach bekanntwerden der Sicherheitslücken ihre Systeme gepatched und neu gestartet.

Weitere Hardware

Neben den Herstellern von Prozessoren haben auch Hersteller anderer Hardware Firmware- und/oder Treiber-Updates veröffentlicht.

Switche, Router und NAS können ebenfalls anfällig für Angriffe sein, da diese häufig über einen Prozessor von Intel, ARM oder Qualcomm verfügen.

Generell sollten nicht nur die Betriebssysteme, sondern nach Möglichkeit auch die anderen Komponenten eines Systems aktualisiert werden, um eine eventuelle Komprimittierung durch Schadsoftware auszuschließen, die die Lücken Meltdown und Spectre ausnutzt.

Quellen, weitere Informationen

Meltdown:
https://meltdownattack.com/meltdown.pdf
Heise Online hat eine Übersicht mit Fragen als FAQ unter diesem Link bereitgestellt:
https://www.heise.de/newsticker/meldung/FAQ-zu-Meltdown-und-Spectre-Was-ist-passiert-bin-ich-betroffen-wie-kann-ich-mich-schuetzen-3938146.html
Intel hat eine Liste aller von Meltdown betroffenen CPUs veröffentlicht:
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
https://meltdownattack.com/meltdown.pdf
Update hier als Beispiel Microsoft:
https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056892
Zusätzlich bieten Hersteller von Mainboards ebenfalls BIOS-Updates für ihre Boards an:
https://www.hardwareluxx.de/index.php/news/hardware/mainboards/45408-meltdown-asus-und-msi-stellen-bios-updates-fuer-z370-mainboards-bereit.html
Intel rät von BIOS-Update ab:
https://www.heise.de/security/meldung/Meltdown-und-Spectre-Intel-zieht-Microcode-Updates-fuer-Prozessoren-zurueck-3948447.html

Spectre 1 und Spectre 2
https://spectreattack.com/spectre.pdf
VMWare und Microsoft haben umgehend mit Updates reagiert:
https://www.vmware.com/security/advisories/VMSA-2018-0004.html
https://vinfrastructure.it/2018/01/meltdown-spectre-vmware-patches/
https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056892

Weitere Hardware
NVIDIA z.B. hat Updates ihrer Grafikkartentreiber veröffentlicht:
http://nvidia.custhelp.com/app/answers/detail/a_id/4609
Die Routerhersteller AVM und Lancom haben bereits in einem Sicherheitshinweis auf Meltdown und Spectre reagiert:
https://avm.de/service/aktuelle-sicherheitshinweise/
https://www.lancom-systems.de/service-support/soforthilfe/allgemeine-sicherheitshinweise/