TÜVRheinland®
Genau. Richtig.

TÜV Rheinland – Sicherheitshinweise – Meltdown & Spectre – 08. Januar 2018

Massive Sicherheitslücken in Prozessoren entdeckt – Was jetzt zu tun ist

Was ist passiert?

Ein internationales Team von Sicherheitsforschern hat schwerwiegende Sicherheitslücken bei Prozessoren entdeckt. Die Schwachstellen in den Chips ermöglichen Angreifern den Zugriff auf sensible Daten wie Passwörter, Nutzerdaten oder vertrauliche Informationen.

Welche Bereiche sind betroffen?

Betroffen sind die meisten Prozessoren, die in Servern bis hin zu Desktop PCs sowie in mobilen Geräten wie Laptops, Smartphones und Tablets verbaut sind. Die Sicherheitslücken befinden sich in vielen Prozessoren, einschließlich denen, die in Apple-Geräten verwendet werden. Eine Reihe von Sicherheitsupdates wurde bereits veröffentlicht.

Warum ist das Problem so massiv?

Die Sicherheitslücken sind auf eine erhebliche Schwachstelle im Design von Computerprozessoren zurückzuführen. Bis jetzt ist ein konkreter Angriff auf diese Schwachstelle noch nicht bekannt, aber es ist nur eine Frage der Zeit, bis Hacker ihn ausnutzen. Die schiere Anzahl der betroffenen Geräte ist so groß, dass sie sich als sehr verlockender Angriffsvektor erweisen, während die Systeme entsprechende angemessene Updates durchlaufen. Quantitativ sind vermutlich Milliarden von Geräten betroffen.

Was genau ist das Problem?

Um die Leistung zu verbessern, können Computerprozessoren spekulativ Codes ausführen oder Schritte unternehmen, um Daten vorzubereiten, die vor der Anforderung durch den Benutzer verarbeitet werden sollen. Während dieser Vorbereitungsphase werden Zugriffsrechte nicht immer überprüft, wodurch eine Lücke im Sicherheitsmodell des Prozessors entsteht, die von einem Angreifer ausgenutzt werden könnte.

Zwei Fehler wurden festgestellt:

- **Meltdown** ermöglicht den Zugriff auf Daten auf einem Prozessor in Bereichen, die in der Regel für normale Benutzersoftware nicht zugänglich sind. Durch den Zugriff auf diesen Bereich könnte der physische Speicher eines Computers untersucht und Daten - einschließlich Passwörtern und geistigem Eigentum wie Prozesssteuerungsdaten oder Anmeldeinformationen für Anlagenadministratoren ausgeschleust werden.
- **Spectre** ermöglicht bestimmten Arten von Programmen, die im so genannten Benutzermodus arbeiten, Daten aus anderen Prozessen auf demselben System zu extrahieren. Dieser Fehler ist nicht einfach zu patchen und erfordert, dass Software mit Gegenmaßnahmen neu kompiliert wird, um Schutz zu bieten.

TÜV Rheinland AG
Am Grauen Stein
51105 Köln
www.tuv.com

Besonderheiten und Bedrohungen für Shared Hosting-Umgebungen

Auf der Grundlage der von Arm, Intel und Google bereitgestellten Informationen bedroht Meltdown / Spectre die Vertraulichkeit von Daten auf Systemen, auf denen Schadsoftware ihren Code lokal ausführen kann. Dies begrenzt die Angriffsvektoren in gewissem Maße. Ein Angreifer muss über Berechtigungen zum Ausführen seines Codes auf dem Computer verfügen, um die Vertraulichkeit zu gefährden.

Wichtig: Die Möglichkeiten, Daten aus dem Speicher auszulesen, ist nicht auf die virtuelle Maschine beschränkt, auf die ein Angreifer Zugriff hat, sondern auch auf den Speicher der zugrundeliegenden physischen Maschine. In Shared Hosting-Umgebungen wie AWS, Google Cloud Platform und Azure wird dies zu einer echten Bedrohung, da sich normalerweise mehrere Unternehmen und Benutzer einen physischen Computer teilen. In einem solchen Fall könnte ein Benutzer Zugriff auf andere Benutzerdaten haben, die im Speicher derselben physischen Maschine gespeichert sind.

Bedrohungen für Clients

Meltdown/Spectre hat auch Auswirkungen auf Client-PCs, da ein normaler Benutzer Daten lesen kann, auf die er normalerweise keinen Zugriff hat. Dies kann zu einer Privilegien-Eskalation auf einer Maschine führen, z.B. wenn es dem Benutzer gelingt, einen NTML-Hash des Speichers der Maschine zu lesen. Mögliche Angriffsvektoren auf Mobiltelefonen sind mit Malware infizierte Apps, die auf Daten anderer Anwendungen oder die des Systems zugreifen. Smartphones könnten durch eine bösartige App kompromittiert werden, die den Datenzugriff mit Meltdown oder Spectre erleichtert.

Die Auswirkungen auf IoT-Geräte

Bei IoT-Geräten ist es selten der Fall, dass ein Angreifer seinen Code überhaupt auf dem System ausführen kann. Darüber hinaus verwenden die meisten IoT-Geräte einfachere CPUs, die von Meltdown / Spectre nicht betroffen sind. Der Angriffsvektor ist also begrenzt.

Prozessoren in IoT-Geräten sind von der aktuellen Sicherheitslücke wahrscheinlich nicht betroffen und zwar aus zwei Gründen:

- IoT-Geräte nutzen keine vorausschauende Daten-Verarbeitung, weil die Rechenleistung des Geräts für die verfügbaren Funktionen ausreicht.

- denn das würde die Energiebilanz verschlechtern, weil möglicherweise Befehle ausgeführt werden, die nicht benötigt werden. Dies wiederum erhöht den Stromverbrauch, der für viele IoT-Geräte wichtig ist.

Wie können Sie Ihre Organisation schützen?

Um zu verhindern, ein Opfer der aktuellen Sicherheitslücken Meltdown oder Spectre zu werden, sollten Unternehmen und insbesondere Betreiber von Industrieanlagen …

1. **... nicht in Panik verfallen.** Das aktuelle Sicherheitsrisiko ist ein weiterer Angriffsvektor unter zahlreichen Möglichkeiten, Geräte und Systeme zu kompromittieren und z.B. Passwörter abzugreifen. Es ist wahrscheinlich, dass Sie Zeit haben, das Problem systematisch anzugehen.

TÜV Rheinland AG
Am Grauen Stein
51105 Köln
www.tuv.com

2. **… umgehend mit dem Patching beginnen.** Die Auswirkungen auf die Prozessor-Performance liegt unter Laborbedingungen bei 5 bis 40 Prozent. Betriebssystem-Patches verzichten erfahrungsgemäß auf Leistungsmerkmale, die eine Sicherheitslücke darstellen.

3. **... Ihr OT-System oder Kontrollsystem prüfen und ermitteln,** ob es von diesen Problemen betroffen sein könnte. **Beachten Sie,** dass die Meltdown-Schwachstelle Berichten zufolge alle seit 1995 außer Betrieb befindlichen Intel-Prozessoren betrifft, einschließlich der seit 2011 verfügbaren x86-64-Intel-CPUs. Prüfen Sie Ihre Prozesssteuerungshardware und sprechen mit Ihrem Systemhaus: Gibt es eine aktuelle Sicherheitswarnung, eine Sicherheits-Empfehlung oder einen aktuellen Patch?

4. **Entscheiden Sie sich** f**ür einen risikobasierten Ansatz,** um Software-Updates oder Patches auf Ihre Anlagenausrüstung anzuwenden. Windows- und Linux-Patches sind jetzt für die Meltdown-Schwachstelle verfügbar, aber die Spectre-Sicherheitslücke ist derzeit nicht patchbar.
   Idealerweise verfügen Sie über eine Patch-Management-Richtlinie, die es Ihnen ermöglicht, gemeldete Probleme zu bewerten und festzustellen, ob ein Patch sofort angewendet oder zu einem späteren Zeitpunkt geplant werden kann.

5. **... über Ihre ERP- oder IT-Systeme nachdenken**, die davon betroffen sein könnten und sicherstellen, dass Ihre IT-Abteilung die notwendigen Patches vornimmt bzw. einen Plan zum Patchen betroffener Systeme erstellt hat.

6. **... Ihre Sicherheitsverantwortlichen anhalten, beim Monitoring von Sicherheitsvorfällen** (Security Analytics) ein besonderes Auge auf geographische Anomalien in Logins zu haben und die Data Leakage Prevention Sensoren entsprechend konfigurieren lassen. Überwachen Sie Ihre Systeme grundsätzlich auf abnormales Verhalten (Indicators of compromise).

7. **...über eine wirksame Tiefenverteidigungsstrategie nachdenken**. Dies beinhaltet unter anderem, aber nicht nur...
   a. ...verschiedene Sicherheitszonen, die sich nicht überschneiden.
   b. ... die ausschließliche Virtualisierung von Systemen auf demselben physischen Host, die ähnliche Daten hinsichtlich ihrer CIA-Anforderungen (Vertraulichkeit, Integrität, Verfügbarkeit) verarbeiten.
   c. Virtualisieren Sie keine Systeme, die hochkritische Daten hosten, z. B. zentrale Authentifizierungssysteme.
   d. Verwenden Sie nie ein und dasselbe Passwort / Zugangsdaten nicht in einer anderen Sicherheitszone (oder Sicherheitsstufen)
   e. Patchen Sie Ihre Systeme regelmäßig.
   f. Es muss ein ordnungsgemäßer und ausgereifter Schwachstellenverwaltungsprozess implementiert sein, der alle Komponenten abdeckt, die mit Servern, Netzwerkkomponenten, Softwarebibliotheken, Firmware usw. beginnen.
   g. Wählen Sie ihre Drittanbieter sorgfältig aus.

8. Nutzen Sie dies als Gelegenheit, um Ihr gesamtes technisches Cybersicherheitsrisiko im operativen Bereich zu überprüfen und sicherzustellen, dass Sie wirksame Prozesse, Richtlinien und Kontrollen implementiert haben, um die Risiken angemessen zu handhaben. Bedenken Sie, dass eine OT Threat Monitoring-Lösung helfen könnte, solche Probleme in Zukunft zu überwachen.

TÜV Rheinland AG
Am Grauen Stein
51105 Köln
www.tuv.com

Vielleicht doch schon ein Opfer – was dann?

Sollten Sie den Verdacht haben, bereits einer Attacke zum Opfer gefallen zu sein, sollten Sie zu einem Partner Ihres Vertrauens für Cyber Security Kontakt aufnehmen, damit er sie mit den erforderlichen Maßnahmen und weitere Untersuchungen unterstützen und den Schaden begrenzen kann.

Sie benötigen Hilfe?

Für unmittelbare Unterstützung kontaktieren Sie bitte einen Ihrer regionalen Partner für Cyber Security.

Nord-Amerika
Mitch Lapidus
Vice President of Sales, OpenSky Corp, TÜV Rheinland Company
Tel: +1 (973) 479-7457
E-Mail: MLapidus@openskycorp.com

Europa
Bjoern Haan
Geschäftsführer Geschäftsfeld Cyber Security, TÜV Rheinland i-sec GmbH
Tel: +49 174 1880240
E-Mail: Bjoern.Haan@i-sec.tuv.com

Mittlerer Osten, Afrika, Asia Pazifik
John Ramesh
Managing Director, TUV Rheinland L.L.C, Oman
Tel: +968 9423 4267
E-Mail: john.ramesh@om.tuv.com

Asia Pazifik, Japan & China
Sandeep Sinha Roy
Vice President of Sales, ICT & BS, TÜV Rheinland Singapore Pte. Ltd., Singapur
Tel: +65 6562 8750 ext 3323
Email: sandeep.sinharoy@tuv.com

TÜV Rheinland AG
Am Grauen Stein
51105 Köln
www.tuv.com