Meltdown und Spectre

Collax Sicherheitsempfehlung

Aktuelle Lage und Kurzbeschreibung (3.5.2018)

Nach einem Bericht der Heise-Security wurden erneut Sicherheitslücken in Intel-Prozessoren gefunden. Alle jüngst aufgetretenen Lücken waren anscheinend bisher unbekannt gewesen.

Zusätzlich werden diese Lücken als noch gravierender eingeschätze, wie die Anfang des Jahres bekanntgewordenen Lücken. Als Namensgebung wurde „Spectre Next Generation“ oder kurz „Spectre NG“ in den Medien gewählt.

Mindestens eine Lücke wird bei der Risikoeinschätzung als kritisch eingestuft, da die Virtualisierungsgrenze überschritten werden kann, und das Wirt-System aus einer VM heraus attackiert werden kann. Gerade für Cloud-Anbieter ist diese Art der Lücke ein sehr großes Sicherheitsproblem.

Am 7. Mai läuft eine Frist von Googles Project Zero ab. Bis dahin könnten Hersteller einen Spectre-NG-Patch bereitstellen, bevor Details zur Lücke veröffentlicht werden. Allerdings ist nicht sicher, ob der Hersteller Intel, und auch Microsoft, oder Linux Distributionen rechtzeitig Patches liefern können.

Quelle: (De) https://www.heise.de/

Beschreibung der Lage im Januar

Wie aus den Medien bekannt: Sicherheitsforscher von Google haben Sicherheitslücken in Prozessoren entdeckt. Diesen Lücken wurden die Namen *Meltdown* und *Spectre* gegeben.

Meltdown ist die Sicherheitslücke, die nicht privilegierten Prozessen das Lesen von Kernel-Memory erlaubt. Meltdown bricht die grundlegendste Isolierung zwischen Benutzeranwendungen und dem Betriebssystem. Dieser Angriff ermöglicht einem Programm den Zugriff auf den Speicher und damit auch auf die Geheimnisse anderer Programme und des Betriebssystems. Ohne Behebung dieser Sicherheitslücke ist es nicht mehr sicher, mit sensiblen Informationen zu arbeiten. Die Möglichkeit besteht, dass Sie Daten verlieren.

Spectre ist die Sicherheitslücke, die ausnutzt, dass CPUs viele Befehle spekulativ im Voraus ausführen (Speculative execution). Spectre bricht sozusagen die Isolierung zwischen verschiedenen Anwendungen. Es nutzt zusätzlich ein anderes Prozessorfeature aus, welches aufgrund verschiedener Gegebenheiten bestimmte Code-Branches Out-of-Order ausführt. Wenn diese Gegebenheiten künstlich erzeugt werden können, lassen sich wie bei Meltdown gesperrte Speicherbereiche auslesen.

Die Lücken betreffen Micro-Prozessoren mit bestimmten Eigenschaften. Dadurch sind Computer, Mobilgeräte, Server und die Cloud betroffen. Originale Informationen die von der Forschergruppe zusammengefasst und veröffentlicht wurden, finden Sie hier:

(EN) https://meltdownattack.com/

Details über den Schweregrad der Sicherheitslücken finden sie hier:

(EN) https://nvd.nist.gov/vuln/detail/CVE-2017-5754
(EN) https://nvd.nist.gov/vuln/detail/CVE-2017-5753
(EN) https://nvd.nist.gov/vuln/detail/CVE-2017-5715

Inwiefern betrifft das Ihre Collax Server?

Da die Sicherheitslücken ermöglichen, dass auf hauptsächlich Intel® CPU- Systemen Speicherbereiche unerlaubt ausgelesen werden können, sind Server-Produkte von Collax betroffen, die auf Intel® CPU-basierenden Hardware-Systemen oder in Virtualisierungsumgebungen betrieben werden. Im Detail betrifft dies Betriebssystemversionen

Spectre NG

- Collax Business Server 7.0.22 und älter
- Collax Security Gateway 7.0.22 und älter
- Collax Groupware Suite 7.0.22 und älter
- Collax Platform Server 7.0.22 und älter

  sowie
- Collax V-Bien, V-Bien Office und Pro 6.5.18 und älter
- Collax V-Cube, V-Cube+ 6.8.14 und älter

Zum jetzigen Kenntnisstand erfordern die Lücken, dass unbekannte oder nicht zertifizierte Software auf den Servern ausgeführt werden muss. Dadurch lässt sich folgende Risikoeinschätzung zu den Collax Produkten erstellen:

Produkt	Betroffene Versionen	Risikobewertung	Bemerkung
Collax V-Bien, V-Cube, V-Cube+	6.5.18 und älter 6.8.14 und älter	Hoch	Virtuelle Maschinen führen möglicherweise schädliche Software aus.
Collax Business Server **Collax Platform Server** **Collax Groupware Suite**	7.0.22 und älter	Mittel	Benutzerzugriffe auf diese Server sind konzeptionell gewollt und möglich. Risiko verringert sich, wenn File-Virenscanner verwendet werden.
Collax Security Gateway	7.0.22 und älter	Niedrig	Direkte Systemzugriffe sind konzeptionell nicht gewollt, nicht zertifizierte Software kann nicht ausgeführt werden.

Meltdown und Spectre (V1 und V2)

- Collax Business Server 7.0.16 und älter
- Collax Security Gateway 7.0.16 und älter
- Collax Groupware Suite 7.0.16 und älter
- Collax Platform Server 7.0.16 und älter

  sowie
- Collax V-Bien, V-Bien Office und Pro 6.5.18 und älter
- Collax V-Cube, V-Cube+ 6.8.14 und älter

Zum jetzigen Kenntnisstand erfordern die Lücken, dass unbekannte oder nicht zertifizierte Software auf den Servern ausgeführt werden muss. Dadurch lässt sich folgende Risikoeinschätzung zu den Collax Produkten erstellen:

Produkt	Betroffene Versionen	Risikobewertung	Bemerkung
Collax V-Bien, V-Cube, V-Cube+	6.5.18 und älter 6.8.14 und älter	Mittel	Virtuelle Maschinen führen möglicherweise schädliche Software aus.
Collax Business Server **Collax Platform Server** **Collax Groupware Suite**	7.0.16 und älter	Niedrig bis Mittel	Benutzerzugriffe auf diese Server sind konzeptionell gewollt und möglich. Risiko verringert sich, wenn File-Virenscanner verwendet werden.
Collax Security Gateway	7.0.16 und älter	Niedrig	Direkte Systemzugriffe sind konzeptionell nicht gewollt, nicht zertifizierte Software kann nicht ausgeführt werden.

Was können Sie zum Schutz der Collax Produkte tun?

Als ersten Schritt stellt Collax die Softwareversionen 7.0.18, 6.8.16 und 6.5.20 mit einem LTS-Kernel zur Verfügung. Hierin ist die Kernel-Page-Table Isolation aktiviert, welche das Kernel Mapping im Usermode verhindert und damit der Memory-Leak durch die CPU nicht möglich ist.

Ab der Collax Server Version 7.0.22 wird eine Funktion gegen Spectre Variant1 und Variant 2 installiert, die im Linux Kernel implementiert wurde. Diese Schutzfunktion ist nicht auf Microcode Updates seitens der Prozessorhersteller angewiesen. Die Version 7.0.22 schütz somit gegen alle Varianten von Meltdown und Spectre.

Für die Spectre NG-Variante liegen zum jetzigen Zeitpunkt noch keine Patches vor.

Collax empfiehlt dringend:

- **Aktualisieren Sie schnellstmöglich alle Ihre Betriebssysteme und Collax Business Server, Collax Security Gateway, Collax Groupware Suite, Collax Platform Server auf die aktuelle Version 7.0.22**
- **Aktualisieren Sie alle Virtualisierungsserver Collax V-Bien auf Version 6.5.20 und Collax V-Cube auf Version 6.8.18**

Für weitere Fragen zu dem Thema wenden Sie sich an das

Collax Support Team

+49 (0) 89-99 01 57-600
support(at)collax.com