Keine Angst vor Spectre und Meltdown

Das ARTEC Betriebssystem AOS ist von den Sicherheitslücken Spectre und Meltdown nicht betroffen. Anwender müssen nichts unternehmen und behalten die volle Leistungsfähigkeit ihres ARTEC-Systems.

Hintergrund: Die Sicherheitslücken Meltdown und Spectre
Wie aus den Medien bekannt, wurden vor kurzem maßgebliche Sicherheitslücken in fast allen aktuellen Prozessoren entdeckt, die derzeit hohe Wellen schlagen. Diese Lücken liegen in Performance-steigernden Maßnahmen der Prozessor-Hersteller begründet: Denn um die aktuellen, hohen Geschwindigkeiten zu erzielen - und alle Teile effizient nutzen zu können - führen fast alle Prozessoren bestimmte Operationen bereits „auf Verdacht“ aus, um diese bei Bedarf schneller liefern zu können. Das heißt, es werden Berechnungen durchgeführt, selbst wenn noch nicht feststeht, ob das Ergebnis der Berechnung überhaupt benötigt wird und ob das Berechnen gegen eingestellte Sicherheitsbarrieren verstößt. (Die notwendigen Sicherheitsprüfungen werden erst durchgeführt, wenn das Ergebnis tatsächlich benötigt wird.) Die Prozessoren speichern hierbei alle aus dem Arbeitsspeicher gelesenen Werte in einem besonders schnellen Zwischenspeicher (Cache) ab.

Die neu entdeckten Angriffstechniken unter Ausnutzung der Sicherheitslücken Meltdown bzw. Spectre zielen nun darauf ab, in diesem Speicher-Umfeld geschützte Dateninhalte zu „erfühlen“, die das Programm eigentlich gar nicht lesen dürfte. Eine interaktive Webseite, die Javascript verwendet, dürfte beispielsweise keine Möglichkeit haben, an anderer Stelle im RAM des Computers befindliche Passwörter, PINs und TANs oder sonstige Inhalte auszulesen. Um dies dennoch zu ermöglichen, wird der Prozessor im Rahmen der Angriffe millionenfach pro Sekunde provoziert, auf Verdacht Arbeiten durchzuführen, die er nicht durchführen darf und letztlich auch nicht durchführen wird. Bei der Ausführung auf Verdacht werden aber bereits Daten im Cache zwischengespeichert, die in Abhängigkeit zu eigentlich geheimen Speicherwerten stehen – und die dort sonst noch nicht verfügbar wären.

Durch ausgeklügelte Timing-Analysen kann der potenzielle Angreifer nun messen, ob der Cache schon entsprechend gefüllt ist. Durch sehr genaues und häufiges Messen kann die Webseite so z.B. Passwörter aus dem Speicher des Computers ermitteln und per Webaufruf an den Angreifer zurücksenden.

Konsequenz: Patches führen zu massiven Performance-Einbußen
Angreifer könnten die aus Performancegründen geschaffenen Möglichkeiten nutzen, um vertrauliche Daten aus dem RAM auszulesen, die aufgrund der bestehenden Sicherheitseinstellungen eigentlich nicht zugänglich sein dürften.

Besonders stark betroffen von diesen Angriffen sind herkömmliche Cloud-Provider, die auf einer einzelnen Hardware vielen verschiedenen Kunden kleine Parzellen zum Rechnen und Verarbeiten von Daten zur Verfügung stellen, sowie virtualisierte Umgebungen. Angriffe drohen zudem aber auch durch das simple Aufrufen einer Webseite mit interaktiven Elementen, die mithilfe der neuen Angriffstechniken den gesamten Speicherinhalt des Computers oder Smartphones ausspähen können. (Im RAM des Computers finden sich beispielsweise kürzlich geöffnete Dokumente, Passwörter, PIN- und TAN-Nummern, etc.)

Potenziell ist darüber hinaus jedes System betroffen, in dem es mehrere Sicherheitsbarrieren gibt und das über einen Kanal verfügt, um die erspähten Daten auch nach außen zu transportieren. (Skripte, die auf interaktiven Webseiten laufen, verfügen über solch einen Kanal – zum Beispiel in Form simpler Formulare - und können Daten von Webservern nachladen bzw. erspähte Geheimnisse zum Angreifer hochladen.)

Die Schutzmechanismen, die derzeit von den Prozessor-Herstellern entwickelt werden, müssen die vorherigen Performance-Optimierungen nun an einigen Stellen gezielt stören, um die möglichen Angriff zu unterbinden. Dies hat jedoch erhebliche Performance-Verluste von bis zu 30 % zur Folge, welche teure Nachinvestitionen nach sich ziehen können.

Der entscheidende Unterschied: Die Architektur von AOS

ARTEC setzt mit Trusted EMA® aus Sicherheitsgründen bereits seit Jahren bewusst auf Trusted-Computing-Technologie und liefert seine Lösungen von Anfang an als hochsichere, sofort einsatzfähige Black Box-Appliances aus. Administratoren müssen sich hierbei um nichts kümmern, da das ARTEC AOS (wie eine Firmware) alle zum Betrieb nötigen Teile in einer maßgeschneiderten, hochwertigen Hardware (Server) verpackt enthält.

Die grundsätzliche Art der aktuellen Sicherheitslücken hat ARTEC in der Entwicklung seiner Produkte immer berücksichtigt. Denn aufgrund der hohen Sensibilität der zu verarbeitenden Daten - insbesondere in geschäftlichen Umgebungen - wurde bewusst nicht in Betracht gezogen, diese mit anderen Systemen auf einer Hardware (z.B. durch Virtualisierung) zu mischen. Aus diesem Grund haben wir stets dedizierte Systeme für unsere Lösungen eingesetzt. Sensible Daten gehören nach unserer Philosophie immer auf dedizierte Systeme.

Auch in den ARTEC Cloud-Lösungen bietet die Trusted-Computing-Technologie einen besonders hohen Schutz, da unsere Appliances selbst bei einem physikalischen Einbruch in das Rechenzentrum oder bei sonstigen Manipulationsversuchen mit einem hochsicheren Tresor gleichzusetzen sind. Zusätzlich verhindern ausgeklügelte Verschlüsselungskonzepte sowie Funktionen wie das Vier-Augen-Prinzip den unerlaubten Zugriff auf sensible Informationen in verschiedensten Szenarien. Die ARTEC Trusted-Computing-Technologie verhindert hierbei im Gegensatz zu anderen Lösungen das Aushebeln der Schutzmechanismen.

Da die EMA®-Module alle auf der gleichen Technologie basieren und sich ausschließlich auf die Verarbeitung von Daten konzentrieren, existiert das eigentliche Problem der neuen Angriffe für EMA®-Anwender nicht: nämlich, dass externer, schädlicher Code oder Skripte über eine Sicherheitsbarriere hinweg Daten auslesen und nach außen übertragen können.

Im inneren Kern der ARTEC-Produktserien beinhaltet die AOS-Firmware natürlich auch Sicherheitsbarrieren, um einzelne Teile voneinander abzuschotten. Diese können jedoch zu keinem Zeitpunkt fremden Code oder Skripte von Angreifern ausführen, um die geschickten Timing-Angriffe, auf denen Spectre und Meltdown basieren, zu ermöglichen. Der einzig kritische Teil, nämlich die Extraktion von Inhalten aus Dokumenten (wie PDF- und Word-Dateien), wurde von ARTEC auch in einer speziellen Sandbox besonders abgesichert. Hierin könnte also ein theoretisches Risiko bestehen. Die Angriffe würden jedoch zwei wesentliche Dinge erfordern: Einen Kanal, über den ermittelte „Geheimnisse“ nach außen übertragen werden könnten sowie eine ausreichend leistungsfähige Skriptsprache, mit der man die Sandboxen umgehen und die geschickten Timing-Analysen und subtilen Provokationen des Prozessors anstoßen könnte. Beides ist in AOS jedoch nicht gegeben: Weder besteht ein Kanal, über den die Analysemodule Daten nach außen transportieren können, noch führt EMA® Word-Makros o.ä. aus.

Das Grundprinzip der AOS-Firmware, besonders sensible Daten auf dedizierten, nicht geteilten und hochsicheren Systemen aufzubewahren, hat sich also für alle ARTEC-Kunden bereits mehrfach ausgezahlt.

Fazit

Weder ARTEC noch unsere Kunden müssen in Bezug auf die Sicherheit der AOS-basierten EMA®-Appliances handeln. ARTEC wird diesbezüglich nach heutigem Kenntnisstand keine besonderen Updates benötigen oder herausbringen.

Alle unsere Kunden behalten die gewohnt hohe Leistungsfähigkeit, für die sie auch bezahlt haben. Die Performance eingesetzter EMA®s muss also nicht mit einem künftigen Update verlangsamt werden, um sich vor diesen Angriffen zu schützen. Ihre Daten sind und bleiben in Ihrer sicheren EMA® geschützt, die durch Trusted-Computing-Technologie grundsätzlich um Klassen besser abgesichert ist als vergleichbare Lösungen.