Sicherheitslücken in vielen Intel-Systemen

Mit dem Security Advisory SA-00086 warnt Intel vor „kritischen“ Sicherheitslücken in der Firmware vieler Desktop-PCs, Notebooks, Tablets, Server und Embedded Systems aus den letzten zwei Jahren. Betroffen sind Computer mit Intel-Prozessoren ab Skylake, also Core i-6000, Core i-7000 (Kaby Lake), Core i-8000 (Coffee Lake), Xeon Scalable Processor, Xeon W sowie die Apollo-Lake-Chips Atom x5-E3900, Celeron N/J 3000 und Pentium N/J 4000.

Die Fehler stecken je nach System in unterschiedlichen Funktionen. Bei den Core i samt den damit verwandten Celerons und Pentiums ist die Management Engine ME 11.0 bis 11.7 betroffen, bei den Xeon-SP/W die Server Platform Services SPS 4.0. Bei den Apollo-Lake-Chips geht es um die Trusted Execution Engine TXE 3.0, nicht zu verwechseln mit Trusted Execution Technology TXT. Für die einzelnen Fehler hat Intel CVE-Codes herausgegeben (CVE-2017-5705 bis 2017-5712). Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor „mehreren Sicherheitslücken“, von denen sich einige auch aus der Ferne nutzen lassen (Remote-Angriff). Unter anderem können sich Angreifer in der ME Administratorrechte verschaffen oder beliebigen Code ausführen.

Intel stellt Software für Windows und Linux bereit, die prüft, ob die Firmware des jeweiligen Rechners betroffen ist. Je nach System lassen sich die Fehler durch ein BIOS-Update beseitigen oder durch ein separates Update nur für die SPS- oder TXE-Firmware. Updates stellen die jeweiligen Hersteller des Mainboards oder Computers bereit. Einige liefern sie bereits, andere wollen nachziehen. Eine Liste mit Links zu Info-Webseiten finden Sie unter ct.de/ybc7.

Die Sicherheitslücken SA-00086 sind bereits das zweite schwerwiegende Problem in Intels ME-Firmware im laufenden Jahr. Bereits am 1. Mai hatte Intel mit SA-00075 zu Updates geraten. SA-00086 hat Intel wenige Wochen vor einem Vortrag der Sicherheitsexperten Mark Ermolov und Maxim Goryachy von der Firma PTE auf der Konferenz Black Hat Europe veröffentlicht. Der Vortragstitel „How to hack a turned-off Computer, or running unsigned Code in Intel Management Engine“ legt Handlungsbedarf nahe.

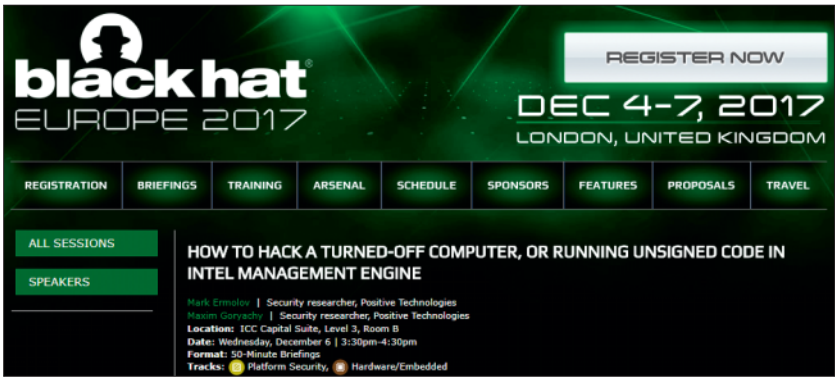
Intels Management Engine wird seit Jahren kritisiert, weil sie als unabhängiges Subsystem mit unvollständig dokumentiertem Funktionsumfang läuft, aber Zugriff auf interne Schnittstellen und Bussysteme hat. Theoretisch kann ein Angreifer, der die ME kapert, Daten via Netzwerkchip aus dem RAM auslesen. Malware, die sich in der ME-Firmware verankert, ist vom Betriebssystem aus unauffindbar und übersteht sowohl Neustarts als auch den Austausch von SSD oder Festplatte.

Intel hält dagegen, dass sich Manipulationen der Firmware durch Zusatzfunktionen wie Boot Guard verhindern ließen. Hacker belegen allerdings immer wieder, dass bei Weitem nicht alle Hersteller von PCs und Mainboards solche Schutzmaßnahmen aktivieren oder dabei Fehler machen.

Bisher gibt es keine Möglichkeit, die Management Engine zuverlässig abzuschalten, ohne die Stabilität des Computers zu gefährden. Es wurden lediglich Firmware-Hacks entdeckt, die Teile der ME deaktivieren; Intel leistet dafür aber keinen Support. Die ME übernimmt beispielsweise Aufgaben beim Booten des Systems. Sie realisiert aber je nach Firmware und Chipsatz auch Funktionen wie die erwähnten SPS und TXE, aber auch Active Management Technology (AMT, Fernwartung bei Q-Chipsätzen und C236), Software Guard Extensions (SGX) und Protected Audio/Video Path (PAVP). *(ciw@ct.de)*

ME-Firmware-Updates: ***ct.de/ybc7***

Anzeige



Über die neuen Sicherheitslücken in Intels ME-Firmware berichten Experten der Firma PTE auf der Black Hat Europe 2017.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover