Erledigt Massive Sicherheitslücke in neueren (ab 2015) Intel Prozessoren

Beitrag von „Si Vis Pacem“ vom 22. November 2017, 09:25

PC vendors scramble as Intel announces vulnerability in firmware

---

Beitrag von „jboeren“ vom 22. November 2017, 09:53

Da freut sich die Geheimdienst bestimmt! 

Beitrag von „Dr.Stein“ vom 22. November 2017, 12:17

Mein Englisch ist nicht so berauschend...was steht da ? Ich mag auch nicht immer auf jeden Link klicken 
Beim nächsten Link Post wäre eine kleine deutsche Zusammenfassung fûr Alle von vorteil.

Beitrag von „matt82“ vom 22. November 2017, 12:25

Angriff:
Bei den ME-Funktionsvarianten "Active Management Technology" (AMT) und "Intel Standard Manageability" (ISM) können Angreifer via Netzwerk höhere Zugriffsrechte erlangen, sofern diese Fernwartungsfunktionen auch eingeschaltet und eingerichtet (provisioned) sind.

Bei der abgespeckten Fernwartung namens "Small Business Advantage" (SBA) lässt sich die Schwachstelle laut Intel glücklicherweise nur von lokalen Angreifern nutzen, die physischen

Zugriff auf ein betroffenes System haben.

Quelle:
https://www.heise.de/security/...en-seit-2010-3700880.html

Beitrag von „ductator“ vom 22. November 2017, 12:26

Zusammendfassend sollen die Lücken wohl Codeausführung erlauben.
BIOS-Updates sind aber schon angekündigt bzw. verfügbar.

Im Grunde genommen ist das eine Wasser ist feucht Meldung. Sowohl die älteren Intel Plattformen, als auch AMD haben da Sicherheitslücken in diesen Firmwareteilen.

Beitrag von „umax1980“ vom 22. November 2017, 12:53

Immer wieder sehr interessant sowas zu lesen, und wo überall und auch aus welchen Gründen nach Sicherheitslücken gesucht wird.

Beitrag von „Altemirabelle“ vom 22. November 2017, 21:27

Die wichtigsten betroffenen:

- Intel Core processors from the 6th generation ("**Skylake**"), 7th generation ("**Kaby Lake** "), & 8th Generation ("**Kaby Lake-R**" and "**Coffee Lake**") families—the processors in most desktop and laptop computers since 2015.

Beitrag von „bernod“ vom 23. November 2017, 08:00

Das müsste doch eigentlich jedem klar sein, dass kein System unangreifbar ist.. und ich als alter "Verschwörungstheoretiker" glaube schon lange nicht mehr daran, dass die Hersteller nicht irgendeinen Deal mit irgendwelchen Organisationen haben, um jederzeit Zugriff auf die Systeme zu haben...