Erledigt Massive Sicherheitslücke in neueren (ab 2015) Intel Prozessoren

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