

Optionales Windows-Update schließt einige Spectre-NG-Lücken

Microsoft stellt über das Windows-Update KB4465065 **neue Microcode-Updates für Intels Core-i- und Xeon-Prozessoren** bereit. Diese hatte Intel bereits im August veröffentlicht. Die Updates schützen unter anderem vor einigen unter der Bezeichnung Spectre NG subsumierten Lücken wie L1 Terminal Fault (L1TF, auch Fore-shadow genannt), Spectre V3a und Spectre V4.

Der Patch KB4465065 für Windows 10 1809 wird allerdings nicht automatisch installiert. Das ist auch nicht unbedingt notwendig, weil Hersteller von PCs, Notebooks und Mainboards die aktualisierten Microcodes in ihre BIOS-Updates einbauen. Enthalten sind Patches für Prozessoren der Serien Core i ab der sechsten Generation (Skylake) und Xeon ab Broadwell (Xeon E5-2000 v4), die Intel seit dem Jahr 2015 verkauft. Bei älteren CPUs

lohnt es deshalb nicht, dieses Windows-Update einzuspielen.

Auch mit installiertem Patch sind nicht alle Schutzfunktionen automatisch



Mit den Microcode-Updates werden CPUs wie der Core i7-6700K wieder etwas sicherer.

aktiv: Speculative Store Bypass Disable (SSBD) gegen Spectre V4 funktioniert erst dann, wenn man es in der Registry unter „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\FeatureSettingsOverride“ aktiviert. Der einzutragende Wert hängt vom Prozessortyp ab. Welcher der richtige ist, erklärt ein Eintrag im Support-Bereich der Microsoft-Webseite (siehe ct.de/yzf1). Bei den meisten Desktop- und Server-Systemen ist SSBD nicht notwendig, weil keine praktischen Spectre-V4-Angriffe bekannt sind, Browser-Updates den wichtigsten Angriffspfad bereits erschweren und der Patch die Performance reduziert.

(chh@ct.de)

Windows-Update KB4465065 herunterladen: ct.de/yzf1

Anzeige