Written by Marco Attard
07 July 2016

Lenovo ThinkPads suffer from an exploit allowing the disabling of write protection of critical firmware areas, security researcher Dymtro "Cr4sh" Oleksiuk warns.

Dubbed "ThinkPwn," the exploit targets a privilege escalation flaw in a Unified Extensible Firmware Interface (UEFI) driver. It allows attackers to remove the flash write protection and execute rogue flaw in the System Management Mode (SMM), a privileged CPU operation mode.

Oleksiuk says the result can disable SecureBoot (prevents boot-level rootkits) and the Windows 10 Credential Guard feature (prevents theft of enterprise domain credentials). And if matters weren't bad enough, the flaw probably comes from a CPU reference specification used by a number of independent BIOS vendors (IBVs), meaning it might also affect laptops from OEMs other than Lenovo.

According to researcher Alex James the vulnerable code is also found in HP and Gigabyte laptops, but it will take a long time before all affected machines are discovered, never mind patched.

In some good news, taking advantage of ThinPwn requires physical access to a target PC, since it needs to be executed from a USB drive as an UEFI application using the UEFI shell. However, according to Oleksiuk says ThinkPwn can be exploited by malware in the near future.

Lenovo has issued an advisory stating it is "engaging all of its IBVs as well as Intel to identify or

rule out any additional instances of the vulnerability's presence in the BIOS provided to Lenovo by other IBVs, as well as the original purpose of the vulnerable code."

Go Lenovo Think Pad Arbitary Code Execution Exploit

Go Lenovo SIMM BIOS Vulnerability Advisory