Issued 9/12/18

Security Flaw in Nearly All Modern PCs and Macs Exposes Encrypted Data

Most modern computers, even devices with disk encryption, are vulnerable to a new attack that can steal sensitive data in a matter of minutes, new research says. In new findings published Wednesday, F-Secure said that none of the existing firmware security measures in every laptop it tested “does a good enough job” of preventing data theft. F-Secure principal security consultant Olle Segerdahl told TechCrunch that the vulnerabilities put “nearly all” laptops and desktops — both Windows and Mac users — at risk. The new exploit is built on the foundations of a traditional cold boot attack, which hackers have long used to steal data from a shut-down computer. Modern computers overwrite their memory when a device is powered down to scramble the data from being read. But Segerdahl and his colleague Pasi Saarinen found a way to disable the overwriting process, making a cold boot attack possible again. It’s no secret that if you have physical access to a computer, the chances of someone stealing your data is usually greater. That’s why so many use disk encryption — like BitLocker for Windows and FileVault for Macs — to scramble and protect data when a device is turned off. But the researchers found that in nearly all cases they can still steal data protected by BitLocker and FileVault regardless. After the researchers figured out how the memory overwriting process works, they said it took just a few hours to build a proof-of-concept tool that prevented the firmware from clearing secrets from memory. From there, the researchers scanned for disk encryption keys, which, when obtained, could be used to mount the protected volume. It’s not just disk encryption keys at risk, Segerdahl said. A successful attacker can steal “anything that happens to be in memory,” like passwords and

corporate network credentials, which can lead to a deeper compromise. Their findings were shared with Microsoft, Apple, and Intel prior to release. According to the researchers, only a smattering of devices aren't affected by the attack. Microsoft said in a recently updated article on BitLocker countermeasures that using a startup PIN can mitigate cold boot attacks, but Windows users with "Home" licenses are out of luck. And, any Apple Mac equipped with a T2 chip are not affected, but a firmware password would still improve protection.