‘Thunderclap’ vulnerability could leave Thunderbolt computers open to attacks

A team of researchers has revealed a new security vulnerability in the Thunderbolt data transfer specification called “Thunderclap” that could leave computers open to serious attacks from otherwise innocuous USB-C or DisplayPort hardware.

As researcher Theo Markettos explains, Thunderclap takes advantage of the privileged, direct-memory access (DMA) that Thunderbolt accessories are granted to gain access to the target device. Unless proper protections are put in place, hackers can use that access to steal data, track files, and run malicious code.

It’s the sort of OS-level access that accessories like GPUs or network cards are typically granted. Because Thunderbolt is designed to replicate those functions externally, it requires the same level of access, but the external nature of the setup makes it more vulnerable to attack. Fundamentally, plugging a malicious device into a port is easier than cracking open someone’s computer and plugging in a hacked graphics card.

Older Thunderbolt devices based on DisplayPort instead of USB-C are also theoretically at risk

The Thunderclap vulnerability isn’t unique to Thunderbolt 3; older Thunderbolt devices based on DisplayPort instead of USB-C are also theoretically at risk.

Markettos and his team discovered the vulnerability in 2016, and have already released it to manufacturers who have been

developing fixes: Apple rolled out a fix for a specific part of the bug in macOS 10.12.4 that same year, and most recently updated Macs should be protected against the attack. Windows 10 version 1803 also protects against the vulnerability on a firmware level for newer devices.

It’s not the sort of attack most users will typically encounter. (Hackers using specially poisoned USB-C devices to target computers by pretending to be a fake GPU usually doesn’t come up for most people.) But it’s a good reminder that you should be careful about plugging your computer into accessories or chargers you don’t trust.

And even if Thunderclap won’t even hit your device, it highlights that even our best standards aren’t perfect, even for the high-end side of the peripherals industry that Thunderbolt represents.

https://www.theverge.com/2019/2/27/18243503/thunderclap-vulnerability-thunderbolt-computers-attack