Thunderbolt flaw allows access to a PC’s data in minutes

Vulnerabilities discovered in the Thunderbolt connection standard could allow hackers to access the contents of a locked laptop’s hard drive within minutes, a security researcher from the Eindhoven University of Technology has announced. *Wired* reports that the vulnerabilities affect all Thunderbolt-enabled PCs manufactured before 2019.

Although hackers need physical access to a Windows or Linux computer to exploit the flaws, they could theoretically gain access to all data in about five minutes even if the laptop is locked, password protected, and has an encrypted hard drive. The entire process can reportedly be completed with a series of off-the-shelf components costing just a few hundred dollars. Perhaps most worryingly, the researcher says the flaws cannot be patched in software, and that a hardware redesign will be needed to completely fix the issues.

Apple’s Macs have offered Thunderbolt connectivity since 2011, but researchers say that they’re only “partially affected” by Thunderspy if they’re running macOS. The result, the report claims, is that macOS systems are vulnerable to attacks similar to BadUSB. This is a security flaw that emerged back in 2014 which can allow an infected USB device to take control of a computer, steal data, or spy on a user.

Björn Ruytenberg, the researcher who discovered the vulnerabilities, has posted a video showing how an attack is performed. In the video, he removes the backplate and attaches a device to the inside of a password-protected Lenovo ThinkPad

laptop, disables its security, and logs in as though he had its password. The whole process takes about five minutes.

[embedded content]

This is not the first time security concerns have been raised about Intel's Thunderbolt technology, which relies on direct access to a computer's memory to offer faster data transfer speeds. In 2019, security researchers revealed a Thunderbolt vulnerability they called "Thunderclap" which allowed seemingly innocuous USB-C or DisplayPort hardware to compromise a device. Security issues like these are reportedly the reason Microsoft hasn't added Thunderbolt connectors to its Surface devices.

In a blog post responding to the report, Intel claims that the underlying vulnerability is not new, and that it was addressed in operating system releases last year. However, *Wired* reports that this Kernel Direct Memory Access Protection has not been universally implemented. The security researchers say they couldn't find any Dell machines with the protection applied, and that they could only verify that some HP and Lenovo laptops used it.

Ultimately, Ruytenberg says that the only way for users to fully prevent against such an attack is for them to disable their computer's Thunderbolt ports in their machine's BIOS, enable hard drive encryption, and turn off their computer when leaving it unattended. The researcher has developed a piece of software called Spycheck (available via the Thunderspy site) that they say should tell you whether your machine is vulnerable to the attack.

Thunderbolt 3 is due to be integrated into the USB 4 specification. Researchers say that USB 4 controllers and peripherals could also be vulnerable and will need to be tested once available.

Update May 5th, 8:07AM ET: *Updated with more details about the*

vulnerabilities in macOS.

https://www.theverge.com/2020/5/11/21254290/thunderbolt-security-vulnerability-thunderspy-encryption-access-intel-laptops