Millions of Thunderbolt-Equipped Devices Open to 'ThunderSpy' Attack

A new attack enables bad actors to steal data from Windows or Linux devices equipped with Thunderbolt ports – if they can get their hands on the device for just five minutes.

The attack, called "Thunderspy," specifically targets Thunderbolt technology, which is a hardware interface developed by Intel (in collaboration with Apple) that allows users to consolidate data transfer, charging and video peripherals into a single connector. While Apple first introduced Thunderbolt ports on its MacBook Pro in 2011, the technology has also been widely adopted with varying PCs such as Dell, HP and Lenovo. Researchers say all Thunderbolt-equipped devices manufactured before 2019 are vulnerable — meaning that there are millions of devices at risk.

To launch the Thunderspy attack, one would need physical access to the device. However, the attack can be launched in minutes, and only involves use of a Thunderbolt-equipped computer, a screwdriver and some portable hardware. Attackers could then bypass security measures and access data — even if the target device is locked and its drive encrypted.

"Thunderspy is stealth, meaning that you cannot find any traces of the attack. It does not require your involvement, i.e., there is no phishing link or malicious piece of hardware that the attacker tricks you into using," said Björn Ruytenberg, a security researcher who is currently a student at the Eindhoven University of Technology, in a Sunday post. "Thunderspy works even if you follow best security practices by locking or suspending your computer when leaving briefly, and if your system administrator has set up the device with Secure Boot, strong BIOS and operating system account passwords, and enabled full disk encryption."

The Attack

Based on a slew of flaws related to Thunderbolt protocol security measures, Ruytenberg developed nine attack scenarios for how the vulnerabilities could be exploited by a malicious entity to access victims' systems – even with the industry standards in place.

The Issue

Thunderbolt ports have historically caused concerns about security over the years. That's because in order to enable high-bandwidth, low-latency use cases (like external graphics cards), the Thunderbolt interface exposes the system's internal PCI Express (PCIe) domain to external devices. Therefore, Thunderbolt devices possess direct memory access (DMA)-enabled I/O, allowing the ability to read and write all of system memory on a PC.

In 2019, researchers disclosed a set of vulnerabilities collectively dubbed "Thunderclap" that put computers at risk from weaponized peripheral devices. Due to Thunderbolt devices' communication via the PCIe protocol, an attacker could abuse the flaw by convincing a user to connect a legitimate – but trojanized – device.

Disclosure

Ruytenberg disclosed the flaws to Intel on Feb. 10. Intel told the researcher it was aware of the flaws and wouldn't be issuing further mitigations beyond kernel DMA protection. The researcher and chip maker exchanged some back and forth regarding the notification of affected parties – Intel only listed five companies that they would inform, Ruytenberg said, though researchers said 11 more OEM/ODMs and the Linux kernel security team needed to be notified.

Intel for its part recommends Thunderbolt port users check with their system manufacturers to determine whether their system has mitigations incorporated.

"For all systems, we recommend following standard security practices, including the use of only trusted peripherals and preventing unauthorized physical access to computers," according to Jerry Bryant, director of communications for Intel Product Assurance and Security in a Sunday disclosure post. "As part of the Security-First Pledge, Intel will continue to improve the security of Thunderbolt technology, and we thank the researchers from Eindhoven University for reporting this to us."

Reference:

https://threatpost.com/millions-thunderbolt-devices-thunderspy-attack/155620/