Vulnerability found in Apple's T2 security chip

7 October 2020, by Bob Yirka

Credit: Pixabay/CC0 Public Domain

Security firm IronPeak has found a vulnerability in Apple's T2 security chip. They claim in a blog post that the vulnerability allows would-be hackers to gain root access to a wide variety of Apple computers.

Back in 2016, Apple introduced the T1 security chip. Its purpose was to serve as a secondary line of defense for Apple computers—Apple referred to the chip as a gatekeeper for certain functions. Two years later, Apple introduced the T2 security chip—it had more functionally and thus more features, which presumably made Apple computers even more secure. Unfortunately, it appears that the T2 security chip, at least according to IronPeak, has a very serious vulnerability of its own—it allows an unauthorized user to gain root access, which gives virtually unlimited access to everything on the computer—everything except user data. But it is also vulnerable to keylogger installation, which could capture the keystrokes of a legitimate user typing passwords, allowing access to user data and to applications such as banking and credit cards. Root access also allows for installing other software, such as programs that send captured data to hackers waiting for it online.

Computers that have the vulnerability include most iMacs made in 2020, recent iMac Pros, Mac minis from 2018 on, Macbook Air computers made after 2018 and Macbook Pros made after 2018. Apple users who want to know if their computer has the vulnerability can check System Information to see if it lists the Apple T2 chip. Even worse for Mac owners, because the vulnerability is hardware-based, there is no patch coming to fix it. Users will likely have little recourse as it appears unlikely that Apple will redesign the T2 chip to work without the vulnerability anytime soon.

There is one piece of good news—the vulnerability is physical, which means a hacker would require either direct access to the computer or indirect physical access, such as through a USB cable. This means that most Apple computer owners are at very low risk. The real risk lies with so-called state actors—people using computers on behalf of government entities. If they are working with sensitive information, they could be at high risk.

More information:
ironpeak.be/blog/crouching-t2-hidden-danger/