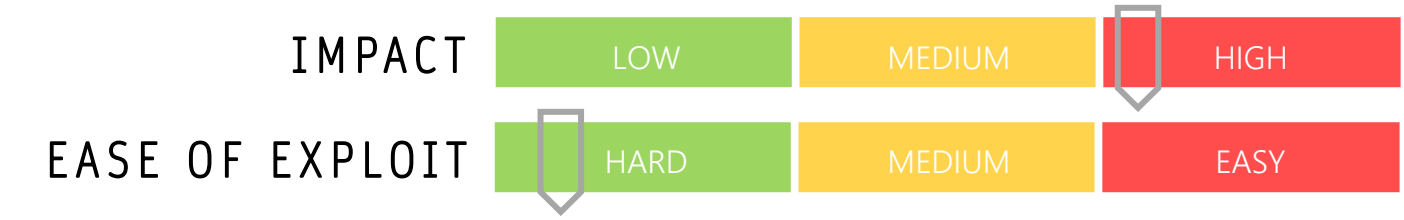
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00051

APPLE T2 CHIP FLAW

DATE ISSUED: 12th October 2020



OVERVIEW

Apple devices containing the T2 chipset and operating macOS are vulnerable to an exploit that allows attackers to gain root access to the system. No patch or fixes have been issued by Apple at this stage.

BREAKDOWN

The 2nd generation Apple chip that sits alongside the main processor as a co-processor and provides additional security features over the prior versions for devices sold between 2018 and 2020. In order to execute the attack, the perpetraitor would need physical access to the device to alter the macOS or load arbitrary kernel extensions to alter the boot sequence or inject hardware. Responsibilities of the Secure Enclave Processor (SEP) is to process sensitive data and perform cryptographic operations as well as TouchID authentication. As this chipset is based on the A10 processor it is open to being exploited by the checkm8 jailbreak hack and another known as the blackbird vulnerability. This is achieved by connecting a USB C cable running v0.11.0 of Checra1n software during boot.

REMEDIATION STEPS

- Use of the FireVault2 as disk encryption means an attacker would have to inject a keylogger into the firmware to alter any of the aforementioned components.
- Be mindful of physical security of your devices and do not allow them to be removed or stolen. Ensure devices are not left unattended.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/apple-t2-flaw-macs/159866/
ZDNet https://www.zdnet.com/article/hackers-claim-they-can-now-jailbreak-apples-t2-security-chip/