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

CYBER GUIDANCE ISSUE 00162

DELL SECURITY BUG REMOTE BIOS RCE ATTACK

DATE ISSUED: 28th June 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	**HARD**	MEDIUM	EASY

OVERVIEW

Four high-severity bugs thought to effect 30 million various Dell devices, including laptops, tablets and desktops, have been discovered that allow attackers to execute arbitrary code in the pre-boot environment by circumventing Secure Boot security standards.

BREAKDOWN

Users with privileged network access are able to sidestep Secure Boot security controls and sabotage the Operating System (OS) and other higher-layer security controls. All four have an 8.3 CVSS rating and affect the BIOSConnect feature that performs firmware updates and remote OS recoveries. This is part of the Dell SupportAssist function preinstalled on all Dell machines preloaded with Microsoft Windows. Attackers are able to exploit the UEFI firmware to access privileged code on the devices remotely. This daisy-chain style attack begins with BIOSConnect attempting an update or recovery by reaching out to backend services for Dell via the Internet. The TLS connection will accept any wildcard certificate which allows attackers to intercept the connection in a Man-in-the-Middle style attack and impersonate the destination, thereafter, sending their own content back to the device (CVE-2021-21571). The second stage of the attack is carried out through the exploitation of any of the overflow vulnerabilities present (CVE-2021-21572, CVE-2021-21573, CVE-2021-21574) to remotely execute their code.

REMEDIATION STEPS

- Install patches issued by Dell immediately.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/dell-bios-attacks-rce/167195/
Dell https://www.dell.com/support/kbdoc/en-nz/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-bios connect-feature-and-https-boot-feature