H-ISAC
HEALTH - ISAC

Dell Boot Recovery Remote Code Execution (RCE) Vulnerability Impacts Millions of Devices

Finished Intelligence Reports | Jun 24, 2021, 09:19 AM

Eclypsium security researchers have discovered a vulnerability in the Dell BIOSConnect feature available on at least 180 models of consumer and business laptops, desktops, and tablets, including devices protected by Secure Boot and Secured-core PCs. This undesignated vulnerability has a calculated CVSS score of 8.3 (High), potentially impacting millions of devices.

The vulnerability can enable an attacker to remotely execute code in the pre-boot environment. Such code may alter the initial state for an operating system, potentially violating common assumptions on the hardware/firmware layers and breaking OS-level security controls.

For a full list of affacted Dell products, please access the Dell advisory, which can be found here.

CVE(s):
CVE-2021-21571
CVE-2021-21572
CVE-2021-21573
CVE-2021-21574

Recommendations:
The system BIOS/UEFI will need to be updated for all affected systems.

- Dell recommends all customers update at the earliest opportunity.
  - When available, customers should apply the BIOS updates for their system. Prior to remediation being applied, Dell recommends customers leverage an alternate method other than BIOSConnect to apply BIOS updates.
- Customers may use one of the Dell notification solutions to be notified and download driver, BIOS and firmware updates automatically once available.
- According to Dell Guidance, users can disable the BIOSConnect feature in either of two ways:
  - Option 1: Customers may disable BIOSConnect from the BIOS setup page (F2).
    - Note: Customers may find the BIOSConnect option under different BIOS setup menu interfaces depending on their platform model. These are referred to below as BIOS Setup Menu Type A and BIOS Setup Menu Type B.
    - BIOS Setup Menu Type A: F2-> Update, Recovery -> BIOSConnect-> Switch to Off
    - BIOS Setup Menu Type B: F2 -> Settings -> SupportAssist System Resolution -> BIOS Connect - >Uncheck BIOSConnect option.

  - Note: Dell recommends customers do not run "BIOS Flash Update - Remote" from F12 until the system is updated with a remediated version of the BIOS.
- Option 2: Customers may leverage Dell Command | Configure (DCC)’s Remote System Management tool to disable the BIOSConnect and Firmware Over the Air (FOTA) BIOS settings.

Release Date: Jun 24, 2021

Sources:

Dell DSA-2021-106: Dell Client Platform Security Update for Multiple Vulnerabilities in the BIOSConnect and HTTPS Boot features as part of the Dell Client BIOS

Eclypsium Discovers Multiple Vulnerabilities Affecting 128 Dell Models via Dell Remote Os Recovery and Firmware Update Capabilities

30M Dell Devices at Risk for Remote BIOS Attacks, RCE

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments: Please email us at toc@h-isac.org

Reference(s)

Dell