مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical “ReVault” Vulnerabilities in Dell ControlVault3 Affecting Business Laptops

Tracking #:432317578

Date:08-08-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Critical “ReVault” Vulnerabilities in Dell ControlVault3 Affecting Business Laptops. These vulnerabilities pose a severe risk to organizations relying on Dell business laptops.

TECHNICAL DETAILS:

Multiple critical vulnerabilities in Dell’s ControlVault3 and ControlVault3+ firmware — a hardware-based security solution used in over 100 actively-supported Dell Latitude and Precision laptop models.

The flaws, collectively dubbed “ReVault”, allow remote and physical attackers to gain persistent access to affected systems, bypass authentication, and extract sensitive credentials — even after a complete Windows reinstallation.

Vulnerability Details:

- **CVE-2025-24311** – Out-of-bounds read/write in firmware
- **CVE-2025-25050** – Out-of-bounds memory access in firmware
- **CVE-2025-25215** – Arbitrary free vulnerability in firmware
- **CVE-2025-24922** – Stack overflow in Windows API
- **CVE-2025-24919** – Unsafe deserialization in Windows API

ControlVault3 is designed to store sensitive authentication data (passwords, cryptographic keys, biometric templates) in a secure, isolated hardware environment.
However, flaws in both the firmware and Windows API components can be exploited to execute arbitrary code, extract cryptographic material, and implant persistent backdoors.

Attack Scenarios

- Remote/Post-Compromise: Non-admin local users can escalate privileges by interacting with vulnerable APIs.
- Physical Access: Attackers can connect to the Unified Security Hub via specialized USB access to bypass security controls.

Risk and Impact:

- Persistence: Attackers can implant malware that survives Windows reinstallation by modifying embedded firmware.
- Credential/Secret Theft: Attackers may extract cryptographic keys, biometric templates, and stored credentials.
- Bypass of Authentication: Physical attackers may tamper with fingerprint authentication, allowing unauthorized entry.
- Detection Avoidance: These attacks operate below the OS, largely undetectable by traditional endpoint security.

Affected Products:

- Dell **Latitude** and **Precision** laptop series (over 100 active models)
- Systems equipped with **ControlVault3** or **ControlVault3+** firmware and Unified Security Hub (USH) boards
- Full list of impacted models is available in Dell’s official advisory **DSA-2025-053**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates released by the Dell.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.dell.com/support/kbdoc/en-us/000276106/dsa-2025-053
- https://blog.talosintelligence.com/revault-when-your-soc-turns-against-you/