ReVault Vulnerabilities in Dell ControlVault3 Firmware Impact Millions of Dell Laptops

TL;DR

Multiple firmware flaws in Dell ControlVault3 and ControlVault3+ affect over 100 laptop models, including widely used Latitude and Precision devices.

Attackers can use these vulnerabilities to backdoor the system, get past Windows login, and trick fingerprint authentication, even after a system wipe. This can be done with either physical access or limited user privileges.

Firmware updates are available and should be applied immediately.

Overview

Multiple vulnerabilities were found in Dell's ControlVault3 and ControlVault3+ firmware, impacting over 100 Dell Latitude and Precision laptop models. These security flaws, which are referred to as ReVault, could allow attackers to gain persistent access to a system, even after the operating system is reinstalled.

Cisco Talos researchers found that attackers can exploit the firmware to bypass Windows authentication, extract sensitive key material, or implant malicious code that survives reboots and OS wipes. The ReVault flaws do not have CVSS scores but affect both the firmware and the Windows APIs in Dell's ControlVault system. ControlVault manages biometric data, passwords, and security keys on a separate hardware module. The five CVEs include:

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

Attackers with physical access or local, non-admin access can exploit these flaws to manipulate the firmware. They can bypass fingerprint validation and install a backdoor without needing OS-level credentials. ReVault creates a pathway for stealthy, low-level persistence that can sidestep operating system controls entirely. Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Patches are available via Dell's support site and Windows Update. You may also see a complete list of impacted products on the site.
- If not in use, turn off fingerprint, smart card, and NFC readers.
- Turn off Fingerprint Unlock when unattended to prevent logins via manipulated firmware.
- Help detect physical tampering attempts by enabling BIOS-level chassis intrusion detection.

TTPs to Watch

Initial Access

- Add Peripheral Device [T1200] – The attacker may use a custom USB connector to access the Unified Security Hub and exploit the firmware without logging into the system.

Credential Access

- Modify Authentication Process: Network Device Authentication [T1556.004] – The attacker may bypass fingerprint authentication by modifying the firmware to accept unauthorized biometric input.

Defense Evasion

- Impair Defenses: Disable or Modify Tools [T1562.001] – The attacker may interfere with endpoint tools or logs to conceal unauthorized firmware changes.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. However, there are some behavioral indicators to watch:

- Unexplained crashes or interruptions in the Windows Biometric Service or Credential Vault Service.
- Unauthorized firmware update attempts detected by endpoint monitoring tools.
- Fingerprint login accepting unregistered prints, especially after system reboots.
- Tamper alerts if chassis intrusion detection is enabled in BIOS.

Aspire is actively monitoring and will notify customers if any IoCs are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These vulnerabilities affect organizations that rely on Dell Latitude and Precision devices, including:

- Government
- Healthcare
- Education
- Finance
- Energy
- Legal
- Defense and Military
- Manufacturing
- Cybersecurity

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will

ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Millions of Dell laptops could be persistently backdoored in ReVault attacks - Help Net Security

ReVault! When your SoC turns against you…