Health-ISAC®
Collaborating for Resilience in Health

VULNERABILITY BULLETINS

Critical ControlVault3 Security Firmware Flaws Discovered impacting Millions of Dell Laptops

TLP:WHITE

Aug 08, 2025

On August 5, 2025, Cisco Talos announced a wide range of vulnerabilities, collectively known as ReVault, affecting over 100 models of Dell laptops, specifically the Latitude and Precision series.

The flaws target the Broadcom BCM5820X security chip within Dell's ControlVault3 (CV) firmware, which is designed to securely store passwords and biometric data. Cisco Talos researchers identified five critical vulnerabilities that allow for potential information leakage, code execution, and firmware modification.

The vulnerabilities have been assigned the following CVEs:

- CVE-2025-24311: An out-of-bounds read vulnerability that enables information leakage
- CVE-2025-25050: An out-of-bounds write flaw allowing code execution
- CVE-2025-25215: An arbitrary memory free vulnerability
- CVE-2025-24922: A stack-based buffer overflow enabling arbitrary code execution
- CVE-2025-24919: An unsafe deserialization flaw in ControlVault’s Windows APIs

This is particularly concerning as attackers could establish persistent undetected access even after a complete operating system reinstallation.

Physical attacks are also possible. An attacker can access the USH board to tamper with the firmware. For example, a compromised laptop's biometric authentication could be modified to accept any fingerprint.

Dell and Broadcom have released firmware updates to address these issues, and customers are urged to apply the patches immediately to versions before ControlVault3 5.15.10.14 and ControlVault3+ 6.2.26.36.

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to these vulnerabilities and take the necessary actions to ensure risk mitigations are implemented, including:

- Keep your system current by regularly updating its firmware. While Windows Update can automatically handle CV firmware, you can often get the newest versions from the Dell website a few weeks earlier.
- If you don't use the security peripherals like the fingerprint reader, smart card reader, or NFC reader, you can disable the related CV services or the CV device itself to enhance security.
- For heightened security, like when you're traveling, consider disabling fingerprint login.
- Windows also offers **Enhanced Sign-in Security (ESS)**, which can help protect against physical attacks and detect unauthorized firmware changes.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	talosintelligence, cybersecuritynews
Vendors	Dell

Release Date
Aug 05, 2025 (UTC)

Alert ID af5952e0

View Alert

Share Feedback
was this helpful? 👍 | 👎

Tags ControlVault3, Vulnerability, Dell, Firmware

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

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App. ▶

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.