May 31, 2024

Overall Rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple Dell vulnerabilities. The Dell PowerStore Family remediation is available for multiple security vulnerabilities that may be exploited by malicious users to compromise the affected system - PowerStore, PowerStore 1000T, PowerStore 1200T, PowerStore 3000T, PowerStore 3200T, PowerStore 5000T, PowerStore 500T, PowerStore 5200T, PowerStore 7000T, PowerStore 9000T, PowerStore 9200T, PowerStoreOS are impacted by this advisory.

Technical Details

PowerStore contain(s) an Improper Certificate Validation Vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to sensitive information leakage via Man in the Middle attack.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-30474, CVE-2024-30475, CVE-2024-30476
- DSA-2024-225: Dell PowerStore Family Security Update for Multiple Vulnerabilities
- VRM Vulnerability Reports