August 16, 2024

Overall Rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a FortiAnalyzer and FortiManager vulnerability. The vulnerability affects Fortinet FortiManager versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, as well as Fortinet FortiAnalyzer versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1

Technical Details

A unverified password change in Fortinet FortiManager and Fortinet FortiAnalyzer may allow an attacker to modify admin passwords via the device configuration backup.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: High
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **MEDIUM** 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 at VulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-21757
- FG-IR-23-467 Privileged admin able to modify super-admins password
- VRM Vulnerability Reports