February 9, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability. The vulnerability affects 6.2.0 through 6.2.15, 6.2.0 through 6.2.15, 6.4.0 through 6.4.14, 7.0.0 through 7.0.13, 7.2.0 through 7.2.6, and 7.4.0 through 7.4.2. Please consult the FortiOS references links below for specific vulnerabilities and versions impacted.

Technical Details

A use of externally controlled format string vulnerability in FortiOS fgfmd daemon CVE-2024-23113 may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests. An out-of-bounds write vulnerability in FortiOS CVE-2024-21762 may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

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

This vulnerability is rated as a **CRITICAL, HIGH, 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.

References

- CVE-2024-23113, CVE-2024-21762, CVE-2023-44487, CVE-2023-47537
- FG-IR-24-029 FortiOS - Format String Bug CVE-2024-23113
- FG-IR-24-015 FortiOS - Out-of-bound Write CVE-2024-21762
- FG-IR-23-397 FortiOS & FortiProxy - CVE-2023-44487 - Rapid Reset HTTP/2 vulnerability CVE-2023-44487
- FG-IR-23-301 FortiOS - Fortilink lack of certificate validation CVE-2023-47537
- Upgrade Path Tool Table
- VRM Vulnerability Reports