November 17, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a FortiSIEM vulnerability. The vulnerability affects FortiSIEM versions 5.4.0, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.2, 5.2.1, 5.1.3, 5.1.2, 5.1.1, 5.1.0, 5.0.1, 5.0.0, 4.10.0, 4.9.0, 4.7.2.

Technical Details

An improper neutralization of special elements used in an OS Command vulnerability in FortiSIEM report server may allow a remote unauthenticated attacker to execute unauthorized commands via crafted API requests.

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

This vulnerability is rated as a **CRITICAL** 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-2023-36553
- PSIRT FG-IR-23-135
- VRM Vulnerability Reports