

## Overall Rating: High



**This is a technical bulletin intended for technical audiences.**

### Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a FortiOS vulnerability. The vulnerability affects FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15 and 6.0 all versions.

### Technical Details

Multiple stack-based buffer overflow vulnerabilities in the command line interpreter of FortiOS may allow an authenticated attacker to execute unauthorized code or commands via specially crafted command line arguments.

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 at [VulnerabilityandRiskManagement@gov.bc.ca](mailto:VulnerabilityandRiskManagement@gov.bc.ca).

### References

- [CVE-2024-23110](#)
- [Multiple buffer overflows in diag npu command](#)
- [VRM Vulnerability Reports](#)