July 9, 2024

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 Fortinet published security advisories to address vulnerabilities in multiple products. Included were updates for the following products:

- FortiADC 7.4 – versions prior to 7.4.1
- FortiADC 7.2 – versions prior to 7.2.4
- FortiADC 7.1 – all versions
- FortiADC 7.0 – all versions
- FortiADC 6.2 – all versions
- FortiADC 6.1 – all versions
- FortiADC 6.0 – all versions
- FortiAIOps 2.0 – versions prior to 2.0.1
- FortiExtender 7.4 – versions prior to 7.4.3
- FortiExtender 7.2 – versions prior to 7.2.5
- FortiExtender 7.0 – versions prior to 7.0.5

Technical Details

Multiple Exposure of sensitive information to an unauthorized actor vulnerabilities [CWE-200] may allow an authenticated attacker to retrieve sensitive information from the API endpoint or logs.

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 VulnerabilityandRiskManagement@gov.bc.ca

References

- CVE-2023-50178 CVE-2024-23663 CVE-2024-27782 CVE-2024-27784 CVE-2024-26006
- Fortinet PSIRT Advisory - FG-IR-22-298
- Fortinet PSIRT Advisory - FG-IR-23-459
- Fortinet PSIRT Advisory - FG-IR-24-069
- Fortinet PSIRT Advisory - FG-IR-24-072
- Fortinet PSIRT Advisories