February 9, 2024

# Cyber Alert

BRITISH COLUMBIA

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

## Summary

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients.  The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

## Technical Details

On February 8, 2024, the Cyber Centre became aware of vulnerabilities impacting multiple versions of Fortinet FortiOS. In response to this advisory the Cyber Centre released advisory AV24-074 on February 9, 2024.

Fortinet reports that CVE-2024-21762 is an out-of-bounds write vulnerability in SSL VPN that may allow a remote unauthenticated threat actor to execute arbitrary code and commands via specially crafted HTTP request. Fortinet has indicated that CVE-2024-21762 may have been exploited in the wild.

A second significant vulnerability (CVE-2024-23113) was reported which is a format string bug within the FortiOS FortiGate to FortiManager (fgfmd) protocol.  The vulnerability may allow a remote, unauthenticated threat actor to execute arbitrary code or commands via specially crafted requests. Fortinet has not indicated that this vulnerability has been exploited.

On February 9, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) updated their Known Exploited Vulnerabilities (KEV) Catalog in response to the Fortinet FortiOS out-of-bound write vulnerability CVE-2024-21762.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk. Fortinet recommends as a temporary workaround, to disable the SSL-VPN service until patching can be completed for CVE-2024-21762. In regard to CVE-2024-23113, Fortinet also recommends that organizations consider whether there is a need to expose the fgfm daemon (port 541) to the internet for inbound connections, until patching can be completed.

## Action Required

The Cyber Centre strongly recommends that organizations determine if any Fortinet devices need to be patched to remediate these vulnerabilities.

| Version | Affected | Solution |
|---|---|---|
| **FortiOS 7.6** | Not affected | Not Applicable |
| **FortiOS 7.4** | 7.4.0 to 7.4.2 | Upgrade to 7.4.3 or above |
| **FortiOS 7.2** | 7.2.0 to 7.2.6 | Upgrade to 7.2.7 or above |
| **FortiOS 7.0** | 7.0.0 to 7.0.13 | Upgrade to 7.0.14 or above |
| **FortiOS 6.4** | 6.4.0 to 6.4.14 | Upgrade to 6.4.15 or above |
| **FortiOS 6.2** | 6.2.0 to 6.2.15 | Upgrade to 6.2.16 or above |
| **FortiOS 6.0** | 6.0 all versions | Migrate to a fixed release |

Organizations should also review and implement the Cyber Centre's Top 10 IT Security Actions with an emphasis on the following topics:

- Consolidating, monitoring, and defending Internet gateways.
- Patching operating systems and applications.
- Isolate web-facing applications

## Partner Reporting

ACSC - Critical Vulnerability in FortiOS
NCSC-NZ - Cyber Security Alert: CVEs affecting FortiOS SSL VPN

## References

- CVE-2024-21762, CVE-2024-23113
- AV24-074 on February 9, 2024
- FortiOS - Out-of-bound Write in sslvpnd
- FortiOS - Format String Bug in fgfmd
- Known Exploited Vulnerabilities Catalog
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- VRM Vulnerability Reports