December 13, 2023

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Fortinet published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- FortiMail – multiple versions
- FortiNDR – multiple versions
- FortiOS – multiple versions
- FortiPAM – multiple versions
- FortiProxy – multiple versions
- FortiPortal – multiple versions
- FortiRecorder – multiple versions
- FortiSwitch – multiple versions
- FortiVoice – multiple versions
- FortiWLM – versions 8.6.0 to 8.6.5

Technical Details

A double free vulnerability [CWE-415] in FortiOS and FortiPAM HTTPSd daemon may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted commands.

Version	Affected	Solution
FortiOS 7.2	Not affected	Not Applicable
FortiOS 7.0	7.0.0 through 7.0.5	Upgrade to 7.0.6 or above
FortiOS 6.4	Not affected	Not Applicable
FortiPAM 1.2	Not affected	Not Applicable
FortiPAM 1.1	1.1.0 through 1.1.1	Upgrade to 1.1.2 or above
FortiPAM 1.0	1.0 all versions	Migrate to a fixed release

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-41678, CVE-2023-36639
- Fortinet PSIRT Advisories