April 9, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended 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 products:

- FortiClientLinux 7.2 – version 7.2.0
- FortiClientLinux 7.0 – versions 7.0.6 to 7.0.10
- FortiClientLinux 7.0 – versions 7.0.3 to 7.0.4
- FortiClientMac 7.2 – versions 7.2.0 to 7.2.3
- FortiClientMac 7.0 – versions 7.0.6 to 7.0.10
- FortiOS – multiple versions
- FortiProxy – multiple versions
- FortiSandbox 4.4 – versions 4.4.0 to 4.4.3
- FortiSandbox 4.2 – versions 4.2.0 to 4.2.6
- FortiSandbox 4.0 – versions 4.0.0 to 4.0.4

Technical Details

- An Improper Control of Generation of Code ('Code Injection') vulnerability [CWE-94] in FortiClientLinux may allow##
  an unauthenticated attacker to execute arbitrary code via tricking a FortiClientLinux user into visiting a malicious website.

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 these risks.

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-2023-45590 CVE-2023-45588 CVE-2024-31492 CVE-2024-23671 CVE-2024-21755 CVE-2024-21756 CVE-2023-41677
- Fortinet PSIRT Advisory - FG-IR-23-087
- Fortinet PSIRT Advisory - FG-IR-23-345
- Fortinet PSIRT Advisory - FG-IR-23-454
- Fortinet PSIRT Advisory - FG-IR-23-489
- Fortinet PSIRT Advisory - FG-IR-23-493
- Fortinet PSIRT Advisories