May 14, 2024

Overall rating: Medium

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

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

- FortiPortal 7.2 – versions 7.2.0 to 7.2.1
- FortiPortal 7.0 – versions 7.0.0 to 7.0.6
- FortiSOAR 7.4 – all versions
- FortiSOAR 7.3 – all versions
- FortiSOAR 7.2 – all versions
- FortiSOAR 7.0 – all versions
- FortiSOAR 6.4 – all versions
- FortiWebManager 7.2 – version 7.2.0
- FortiWebManager 7.0 – versions 7.0.0 to 7.0.4
- FortiWebManager 6.3 – version 6.3.0
- FortiWebManager 6.2 – versions 6.2.3 to 6.2.4
- FortiWebManager 6.0 – version 6.0.2
- FortiSandbox 4.4 – versions 4.4.0 to 4.4.4
- FortiSandbox 4.2 – versions 4.2.0 to 4.2.6

Technical Details

A stack-based buffer overflow [CWE-121] vulnerability in FortiOS administrative interface may allow a privileged attacker to execute arbitrary code or commands via crafted HTTP or HTTPs requests.

What Customers Should Do

Customers who do not wish to use the "Open SSH Console" functionality may remove the PuTTY component completely. Customers who wish to maintain the existing usage of PuTTY should replace the version installed on their XenCenter system with an updated version (with a version number of at least 0.81).

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required

This vulnerability is rated as a **MEDIUM** 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.

References

- CVE-2023-46714 CVE-2023-44247 CVE-2023-41677 CVE-2024-26007 CVE-2023-36640 CVE-2023-45583
- Fortinet PSIRT Advisories