November 15, 2023

Overall rating: Critical

BRITISH COLUMBIA

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

Summary

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

- FortiADC – multiple versions
- FortiGate FGT_VM64_KVM – multiple versions
- FortiSIEM – multiple versions
- FortiWAN – multiple versions
- FortiWLM – multiple versions

Technical Details

A heap-based buffer overflow flaw was found in the SOCKS5 proxy handshake in the Curl package. If Curl is unable to resolve the address itself, it passes the hostname to the SOCKS5 proxy. However, the maximum length of the hostname that can be passed is 255 bytes. If the hostname is longer, then Curl switches to the local name resolving and passes the resolved address only to the proxy. The local variable that instructs Curl to "let the host resolve the name" could obtain the wrong value during a slow SOCKS5 handshake, resulting in the too-long hostname being copied to the target buffer instead of the resolved address, which was not the intended behavior.

These vulnerabilities are rated as an overall **Critical** 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-2023-38545, CVE-2023-41841
- Fortinet PSIRT Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts