April 10, 2024

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 that Palo Alto Networks published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- PAN-OS 11.1 – versions prior to 11.1.2
- PAN-OS 11.0 – multiple versions
- PAN-OS 10.2 – multiple versions
- PAN-OS 10.1 – multiple versions
- PAN-OS 10.0 – versions prior to 10.0.12
- PAN-OS 9.1 – multiple versions
- PAN-OS 9.0 – multiple versions
- PAN-OS 8.1 – versions prior to 8.1.24

Technical Details

A memory leak exists in Palo Alto Networks PAN-OS software that enables an attacker to send a burst of crafted packets through the firewall that eventually prevents the firewall from processing traffic. This issue applies only to PA-5400 Series devices that are running PAN-OS software with the SSL Forward Proxy feature enabled.

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-2024-3382 CVE-2024-3383 CVE-2024-3384 CVE-2024-3385 CVE-2024-3386 CVE-2024-3387 CVE-2024-3388
- Palo Alto Networks Security Advisory - CVE-2024-3382
- Palo Alto Networks Security Advisory - CVE-2024-3383
- Palo Alto Networks Security Advisory - CVE-2024-3384
- Palo Alto Networks Security Advisory - CVE-2024-3385
- Palo Alto Network Security Advisories