December 14, 2023

**Overall Rating - High**

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

## Summary

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

- PAN-OS 11.0 – versions prior to 11.0.1
- PAN-OS 10.2 – versions prior to 2.4
- PAN-OS 10.1 – versions prior to 10.1.9
- PAN-OS 10.0 – versions prior to 10.0.12
- PAN-OS 9.1 – versions prior to 9.1.16
- PAN-OS 9.0 – versions prior to 9.0.17
- PAN-OS 8.1 – versions prior to 8.1.25

## Technical Details

A DOM-Based cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a remote attacker to execute a JavaScript payload in the context of an administrator's browser when they view a specifically crafted link to the PAN-OS web interface.

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-2023-6790
- Palo Alto Networks Security Advisory - CVE-2023-6790
- Palo Alto Network Security Advisories