July 10, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released Palo Alto Networks security advisory to address a critical vulnerability in the following product:

- Palo Alto Networks Expedition – versions prior to 1.2.92

Technical Details

Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition.

Note: Expedition is a tool aiding in configuration migration, tuning, and enrichment. Configuration secrets, credentials, and other data imported into Expedition is at risk due to this issue.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- **CVE-2024-5910** CVE-2024-5911 CVE-2024-5912 CVE-2024-5913 CVE-2024-3596
- **Palo Alto Networks Security Advisory - CVE-2024-5910**
- **Palo Alto Network Security Advisories**