AL2024_16 Palo Alto Networks Patches Critical Flaw in Expedition Migration Tool (15th July 2024)

Description

Palo Alto Networks has recently addressed several critical security vulnerabilities in its products, including an authentication bypass flaw in the Expedition migration tool (CVE-2024-5910) and a RADIUS protocol vulnerability dubbed BlastRADIUS (CVE-2024-3596).

Attack Details

Two critical vulnerabilities have been identified in Palo Alto Networks' products, prompting immediate security updates. The first, CVE-2024-5910, affects the Expedition migration tool by allowing unauthorized access to administrative accounts due to missing authentication. This flaw, present in all versions of Expedition prior to 1.2.92, poses risks of admin account takeovers and exposure of imported configuration secrets and credentials. The second vulnerability, CVE-2024-3596, impacts PAN-OS firewalls using the RADIUS protocol with CHAP or PAP authentication. It enables attackers to conduct adversary-in-the-middle attacks, potentially escalating privileges to 'superuser' level. Affected PAN-OS versions range from 9.1 to 11.1, emphasizing the importance of applying recommended patches promptly to mitigate these security risks.

Recommendations

1. **Expedition Migration Tool (CVE-2024-5910):**
   - Upgrade Expedition to version 1.2.92 or later to mitigate the vulnerability.
   - Restrict network access to Expedition to authorized users, hosts, or networks as a temporary workaround.
2. **BlastRADIUS Vulnerability (CVE-2024-3596):**
   - Upgrade PAN-OS to the fixed versions (details provided in the advisory).
   - Avoid using CHAP or PAP authentication without an encrypted tunnel (use TLS).
   - Consider using EAP-TTLS with PAP as an alternative configuration.

Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (2024, July 11). Palo Alto Networks patches a critical flaw in Expedition migration tool. Retrieved from The Hacker News. https://thehackernews.com/2024/07/palo-alto-networks-patches-critical.html
- Palo Alto Networks Security Advisories. (n.d.). https://security.paloaltonetworks.com/