مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Palo Alto Networks Expedition Migration Tool

Tracking #:432316718

Date:09-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Palo Alto Networks has issued a security advisory addressing multiple vulnerabilities in its Expedition migration tool. These vulnerabilities could expose sensitive data and allow unauthorized actions on affected systems.

TECHNICAL DETAILS:

Expedition, formerly known as the Migration Tool, is a free utility designed to assist organizations in transitioning to Palo Alto Networks' next-generation firewall (NGFW) platform. The tool reached its End of Life (EoL) on December 31, 2024, and is not intended for production environments.

Vulnerabilities Details:

- **SQL Injection (CVE-2025-0103)**
  - **Severity:** High (CVSS 7.8)
  - **Description:** Authenticated attackers can exploit this flaw to access database contents, including password hashes and device API keys. The vulnerability also allows for the creation and reading of arbitrary files on the system, potentially compromising sensitive configuration data.
- **Reflected Cross-Site Scripting (XSS) (CVE-2025-0104)**
  - **Severity:** Medium (CVSS 4.7)
  - **Description:** Attackers can execute malicious JavaScript in a user's browser by tricking them into clicking a crafted link. This could facilitate phishing attacks or session theft.
- **Arbitrary File Deletion (CVE-2025-0105)**
  - **Severity:** Low (CVSS 2.7)
  - **Description:** Unauthenticated attackers could delete files accessible to the www-data user, potentially disrupting critical functions. The impact could escalate in certain environments.
- **Wildcard Expansion Enumeration (CVE-2025-0106)**
  - **Severity:** Low (CVSS 2.7)
  - **Description:** Attackers can enumerate files on the host system, exposing metadata and enabling subsequent attacks.
- **OS Command Injection (CVE-2025-0107)**
  - **Severity:** Low (CVSS 2.3)
  - **Description:** Authenticated attackers can execute arbitrary OS commands on the host, exposing cleartext passwords, usernames, and API keys for PAN-OS firewalls.

Affected Versions:

- Palo Alto Networks Expedition (all versions prior to 1.2.101)

Fixed Versions:

- Palo Alto Networks Expedition version 1.2.101 or later

Note: Palo Alto Networks strongly advises transitioning away from Expedition due to its EoL status.

RECOMMENDATIONS:

Palo Alto Networks recommends transitioning away from the Expedition tool due to its EoL status. For organizations still using Expedition, the following measures are advised:

- **Apply Updates:**
  - Upgrade to Expedition version 1.2.101 or later to address these vulnerabilities.
- **Restrict Access:**
  - Limit access to the tool to authorized users, hosts, and networks only.
- **Shutdown When Idle:**
  - Disable Expedition entirely when not actively in use to reduce exposure.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://security.paloaltonetworks.com/PAN-SA-2025-0001