مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Command Injection Vulnerability in Palo Alto Networks PAN-OS

Tracking #:432317386

Date:17-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Palo Alto Networks PAN-OS that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-4230**
- Severity: Medium (CVSS 5.7)
- A command injection vulnerability exists in Palo Alto Networks PAN-OS software, allowing authenticated administrators with CLI access to bypass system restrictions and execute arbitrary commands as the root user.
- Successful exploitation of this vulnerability could enable an authenticated administrator to execute arbitrary commands with root privileges, potentially resulting in system compromise, data exfiltration, or service disruption.

Affected Version	Affected Minor Version	Remediation
PAN-OS 11.2	11.2.0 through 11.2.5	Upgrade to 11.2.6 or later.
PAN-OS 11.1	11.1.0 through 11.1.9	Upgrade to 11.1.10 or later.
PAN-OS 10.2	10.2.0 through 10.2.13	Upgrade to 10.2.14 or later.
PAN-OS 10.1	10.1.0 through 10.1.14	Upgrade to 10.1.14-h15 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Palo Alto Networks.

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/CVE-2025-4230