مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability Palo Alto Networks PAN-OS

Tracking #:432316894

Date:21-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Palo Alto Networks has disclosed a high-severity vulnerability in the PAN-OS software, affecting the management web interface, has been actively exploited in wild.

TECHNICAL DETAILS:

Palo Alto Networks has disclosed a high-severity vulnerability in the PAN-OS software, affecting the management web interface, has been actively exploited in wild. This vulnerability, which allows authenticated attackers to read files on the PAN-OS filesystem, has been actively exploited in the wild, particularly when chained with other vulnerabilities (CVE-2025-0108 and CVE-2024-9474).

Vulnerability Description:
CVE-2025-0111 is an authenticated file read vulnerability in the PAN-OS management web interface. An attacker with low privileges and network access to the management interface can exploit this vulnerability to read files on the PAN-OS filesystem that are accessible by the "nobody" user. This could potentially expose sensitive configuration files, logs, or other critical system information.

Exploitation Status:

Palo Alto Networks has observed active exploitation attempts involving this vulnerability, often chained with CVE-2025-0108 and CVE-2024-9474. Organizations with unpatched and unsecured PAN-OS management interfaces are at the highest risk.

Version	Minor Version	Suggested Solution
PAN-OS 10.1	10.1.0 through 10.1.14	Upgrade to 10.1.14-h9 or later
PAN-OS 10.2	10.2.0 through 10.2.13	Upgrade to 10.2.13-h3 or later
	10.2.7	Upgrade to 10.2.7-h24 or 10.2.13-h3 or later
	10.2.8	Upgrade to 10.2.8-h21 or 10.2.13-h3 or later
	10.2.9	Upgrade to 10.2.9-h21 or 10.2.13-h3 or later
	10.2.10	Upgrade to 10.2.10-h14 or 10.2.13-h3 or later
	10.2.11	Upgrade to 10.2.11-h12 or 10.2.13-h3 or later
	10.2.12	Upgrade to 10.2.12-h6 or 10.2.13-h3 or later
PAN-OS 11.0 (EoL)		Upgrade to a supported fixed version
PAN-OS 11.1	11.1.0 through 11.1.6	Upgrade to 11.1.6-h1 or later
	11.1.2	Upgrade to 11.1.2-h18 or 11.1.6-h1 or later
PAN-OS 11.2	11.2.0 through 11.2.4	Upgrade to 11.2.4-h4 or later

RECOMMENDATIONS:

- **Upgrade PAN-OS:** Apply the latest fixed versions for affected PAN-OS releases as outlined in the advisory.
- **Restrict Management Interface Access:** Ensure the management interface is accessible only from trusted internal IP addresses.

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-2025-0111