مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Reflected Cross-Site Scripting Vulnerability in PAN-OS GlobalProtect

Tracking #:432317297

Date:22-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Palo Alto Networks has disclosed a reflected cross-site scripting (XSS) vulnerability affecting the GlobalProtect gateway and portal in PAN-OS.

TECHNICAL DETAILS:

Palo Alto Networks has disclosed a reflected cross-site scripting (XSS) vulnerability (CVE-2025-0133) affecting the GlobalProtect gateway and portal in PAN-OS. This vulnerability allows an attacker to craft a malicious URL that, when clicked by an authenticated user accessing a Captive Portal, can execute arbitrary JavaScript in the user's browser. A proof-of-concept is publicly available, increasing the likelihood of exploitation.

Vulnerability Details:

- CVE ID: CVE-2025-0133
- Without Clientless VPN- CVSS-BT: 2.0 /CVSS-B: 5.1 LOW
- With Clientless VPN enabled, there are inherent risks that facilitate credential stealing CVSS-BT: 5.5 /CVSS-B: 6.9 MEDIUM
- Vulnerability Type: Reflected XSS
- Attack Vector: Network
- Exploitability: Proof-of-Concept available

Version	Minor Version	Suggested Solution
PAN-OS 11.2	11.2.0 through 11.2.6	Upgrade to 11.2.7 or later [ETA June 2025]
PAN-OS 11.1	11.1.0 through 11.1.10	Upgrade to 11.1.11 or later [ETA July 2025]
PAN-OS 10.2	10.2.0 through 10.2.16	Upgrade to 10.2.17 or later [ETA August 2025]
PAN-OS 10.1	10.1.0 through 10.1.14	Upgrade to 10.2.17 or later [ETA August 2025]
All other older unsupported PAN-OS versions		Upgrade to a supported fixed version

RECOMMENDATIONS:

- Upgrade PAN-OS to the fixed versions (when released).
- Disable Clientless VPN if not strictly necessary.

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-2025-0133