مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Palo Alto Networks GlobalProtect

Tracking #:432317613

Date:19-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Palo Alto Networks' GlobalProtect VPN application that could allow attackers to escalate privileges and install malicious software on affected endpoints through improper certificate validation.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-2183**
- CVSS v3.1 Score: 4.5 (Medium)
- A security vulnerability has been identified in Palo Alto Networks' GlobalProtect VPN client. The flaw arises from insufficient validation of server certificates, enabling an attacker on the same network segment to redirect GlobalProtect traffic to a malicious server and install fraudulent root certificates. Once installed, these certificates could be leveraged to deploy malicious software signed with attacker-controlled certificate authorities, effectively bypassing security mechanisms.
- Exploitation of this vulnerability can lead to:
  - Unauthorized installation of root certificates
  - Execution of malicious, attacker-signed software
  - Potential bypass of endpoint defenses that rely on code signing validation

Fixed Versions:

- For Windows: Upgrade to 6.3.2-h9 or 6.3.3-h2 or later. 6.2.8-h3 or later.
- For Linux: Upgrade to 6.3.3 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed or latest security updates 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-2025-2183