مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Palo Alto GlobalProtect Application

Tracking #:432317476

Date:11-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Palo Alto released updates, addressing multiple moderate severity vulnerabilities in its GlobalProtect Application.

TECHNICAL DETAILS:

Palo Alto has released two security advisories addressing vulnerabilities in its GlobalProtect Application. The vulnerabilities could allow a locally authenticated non-administrative user to escalate privileges to root or SYSTEM, or disable the GlobalProtect App even when configuration settings should prevent it.

Vulnerability Details:

- **CVE-2025-0140 GlobalProtect App: Non-Admin User Can Disable the GlobalProtect App**
  - **Description:** An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect App on macOS and Linux devices enables a locally authenticated non administrative user to disable the app even if the GlobalProtect app configuration would not normally permit them to do so.
  - **CVSS Score:** 4.3
  - **Severity:** Medium
  - **Configuration for Exposure:** No special configuration is required to be vulnerable to this issue.
  - **Exploitation Status**: Palo Alto Networks is not aware of any malicious exploitation of this issue.
  - **Weakness Type and Impact:**
    - CWE-266: Incorrect Privilege Assignment
    - CAPEC-578 Disable Security Software

- **CVE-2025-0141 GlobalProtect App: Privilege Escalation (PE) Vulnerability**
  - **Description:** An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect App on enables a locally authenticated non administrative user to escalate their privileges to root on macOS and Linux or NT AUTHORITY\SYSTEM on Windows.
  - **CVSS Score:** 5.7
  - **Severity:** Medium
  - **Configuration for Exposure:** No special configuration is required to be vulnerable to this issue.
  - **Exploitation Status**: Palo Alto Networks is not aware of any malicious exploitation of this issue.
  - **Weakness Type and Impact:**
    - CWE-426 Untrusted Search Path
    - CAPEC-233 Privilege Escalation

Affected/Unaffected Versions:

CVE	Versions	Affected	Unaffected
CVE-2025-0140	GlobalProtect App	None on Android	All on Android
		None on Chrome OS	All on Chrome OS
		None on iOS	All on iOS
		None on Windows	All on Windows
	GlobalProtect App 6.3	< 6.3.3-h1 (6.3.3-c650) on macOS	>= 6.3.3-h1 (6.3.3-c650) on macOS
	GlobalProtect App 6.2	< 6.2.8-h2 (6.2.8-c243) on macOS	>= 6.2.8-h2 (6.2.8-c243) on macOS
		< 6.2.8 on Linux	>= 6.2.8 on Linux (ETA: July 11
			2025)
	GlobalProtect App 6.1	All on macOS	None on macOS
		All on Linux	None on Linux
	GlobalProtect App 6.0	All on macOS	None on macOS
		All on Linux	None on Linux
	GlobalProtect UWP App	None	All
CVE-2025-0141	GlobalProtect App	None on Android	All on Android
		None on Chrome OS	All on Chrome OS
		None on iOS	All on iOS
	GlobalProtect App 6.3	< 6.3.3-h1 (6.3.3-c650) on macOS	>= 6.3.3-h1 (6.3.3-c650) on macOS
		< 6.3.3-h1 (6.3.3-c650) on Windows	>= 6.3.3-h1 (6.3.3-c650) on Windows
	GlobalProtect App 6.2	< 6.2.8-h2 (6.2.8-c243) on macOS	>= 6.2.8-h2 (6.2.8-c243) on macOS
		< 6.2.8-h2 (6.2.8-c243) on Windows	>= 6.2.8-h2 (6.2.8-c243) on Windows
		< 6.2.8 on Linux	>= 6.2.8 on Linux (ETA: July 11
			2025)
	GlobalProtect App 6.1	All on macOS	None on macOS
		All on Windows	None on Windows
		All on Linux	None on Linux
	GlobalProtect App 6.0	All on macOS	None on macOS
		All on Windows	None on Windows
		All on Linux	None on Linux
	GlobalProtect UWP App	None	All

RECOMMENDATIONS:

The UAE Cyber Security Council recommends referring to the advisories released by Palo Alto, and applying the necessary updates at the earliest.

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-2025-0140
- https://security.paloaltonetworks.com/CVE-2025-0141