مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in Palo Alto Networks GlobalProtect App

Tracking #:432317369

Date:12-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the GlobalProtect App on macOS that could be exploited to escalate privileges to root, potentially leading to full system compromise.

TECHNICAL DETAILS:

Palo Alto Networks has identified a critical vulnerability, CVE-2025-4232, affecting its GlobalProtect app on macOS. This vulnerability, an improper neutralization of wildcards in the log collection feature, allows an authenticated, non-administrative user to escalate their privileges to root.

Vulnerability Details:

- **CVE-2025-4232**
- CVSS Score 7.1 HIGH
- An improper neutralization of wildcards vulnerability exists in the log collection feature of Palo Alto Networks GlobalProtect app on macOS. This flaw can be exploited by an authenticated, non-administrative user to execute arbitrary code with root privileges.
- Successful exploitation of this vulnerability could allow an authenticated, non-administrative user to achieve Privilege Escalation to Root. This means an attacker can gain complete control over the affected macOS system, enabling them to install programs, view, change, or delete data, and create new accounts with full user rights.

Affected Versions	Affected Minor Version	Fixed Versions
GlobalProtect App 6.3 on macOS	6.3.0 through 6.3.2	Upgrade to 6.3.3 or later.
GlobalProtect App 6.2 on macOS	6.2.0 through 6.2.8-h2	Upgrade to 6.2.8-h2 [ETA June 2025] or 6.3.3 or later.
GlobalProtect App 6.1 on macOS		Upgrade to 6.2.8-h2 [ETA June 2025] or 6.3.3 or later.
GlobalProtect App 6.0 on macOS		Upgrade to 6.2.8-h2 [ETA June 2025] or 6.3.3 or later

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-2025-4232