



AVIS DE SECURITE

Objet	Vulnérabilité critique dans GlobalProtect de Palo Alto
Niveau de criticité	IMPORTANT
Référence	SNCSIRT-2025-ADS-157
TLP	WHITE

Résumé

Une vulnérabilité critique (CVE-2025-4232) a été corrigée dans la fonctionnalité de collecte des journaux de l'application GlobalProtect sur macOS. Cette faille repose sur une mauvaise neutralisation des caractères génériques (wildcards) dans les chemins de fichiers, ce qui permet à un utilisateur local non administrateur d'exécuter des commandes malveillantes avec des privilèges d'administrateur « root ».

Risque de sécurité

- Exécution de code arbitraire
- Accès à des données confidentielles

Systèmes affectés

- GlobalProtect App 6.3 sur macOS version antérieure à 6.3.3,
- GlobalProtect App 6.2 sur macOS version antérieure à 6.2.8-h2,
- GlobalProtect App 6.1 sur macOS,
- GlobalProtect App 6.0 sur macOS.

Recommandations

- Se référer au Bulletin de sécurité de Palo Alto du 11 Juin 2025 pour appliquer les mises à jour : <https://security.paloaltonetworks.com/CVE-2025-4232>