DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 01-06-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans Palo Alto Networks GlobalProtect VPN
Réference	1481
Date de Publication	2026-06-01
Sévérité	Critique

IMPACT :

- Contournement d'authentification
- Accès non autorisé au réseau interne
- Exécution de code à distance possible
- Risque élevé de compromission complète du périmètre

SYSTÉME AFFECTÉ :

- Palo Alto Networks PAN-OS versions 9.1, 10.1, 10.2, 11.0 et 11.1 (certaines builds)

- GlobalProtect VPN (Portal et Gateway)

DÉSCRIPTION :

Une vulnérabilité critique a été découverte dans le composant GlobalProtect VPN de Palo Alto Networks, identifiée sous le nom **CVE-2026-0257** (score CVSS : 9.8). Cette faille permet à un attaquant non authentifié d'exploiter une vulnérabilité dans le processus d'authentification, permettant de contourner les contrôles d'accès et d'obtenir un accès réseau interne.

L'exploitation active de cette vulnérabilité a été observée en environnement réel depuis le 17 mai 2026.

SOLUTION :

- Mettre à jour immédiatement vers une version corrigée (consulter le bulletin officiel Palo Alto).
- Désactiver temporairement GlobalProtect Portal/Gateway si la mise à jour n'est pas possible immédiatement.
- Renforcer la surveillance des logs GlobalProtect.

DOCUMENTATION :

- **CVE-2026-0257 (NVD)** : https://www.cve.org/CVERecord?id=CVE-2026-0257
- **Bulletin officiel Palo Alto Networks** : https://security.paloaltonetworks.com/CVE-2026-0257