ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilité affectant Zyxel Firewalls
Numéro de Référence	60790602/26
Date de publication	06 février 2026
Risque	Important
Impact	Important

Systèmes affectés

- ATP versions ZLD V5.35 jusqu'à V5.41
- USG FLEX versions ZLD V5.35 jusqu'à V5.41
- USG FLEX 50(W)/ USG20(W)-VPN versions ZLD V5.35 jusqu'à V5.41

Identificateurs externes

- CVE-2025-11730

Bilan de la vulnérabilité

Zyxel annonce la correction d'une vulnérabilité affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant authentifié d'exécuter des commandes système.

Solution

Veuillez se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Exécution de commandes système

Référence

Bulletin de sécurité de Zyxel :

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-the-ddns-configuration-cli-command-of-zld-firewalls-02-05-2026