ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les équipements réseau ZyXEL
Numéro de Référence	61362402/26
Date de Publication	24 Février 2025
Risque	Important
Impact	Important

Systèmes affectés

- 4G LTE/5G NR CPE :
  - LTE3301-PLUS versions antérieures à 1.00(ABQU.9)C0
  - FWA505 versions antérieures à 1.60(ACKO.2)V0
  - FWA510 versions antérieures à 1.60(ACGD.0)C0
  - FWA515 versions antérieures à 1.60(ACPZ.0)V0
  - FWA710 versions antérieures à 1.60(ACGC.1)V0
  - Nebula LTE3301-PLUS versions antérieures à 1.18(ACCA.6)V0
- DSL / Ethernet CPE :
  - DX3300-T0 versions antérieures à 5.50(ABVY.7.1)C0
  - DX3300-T1 versions antérieures à 5.50(ABVY.7.1)C0
  - DX4510-B0 versions antérieures à 5.17(ABYL.10.1)C0
  - DX4510-B1 versions antérieures à 5.17(ABYL.10.1)C0
  - DX5401-B1 versions antérieures à 5.17(ABYO.7.1)C0
  - EMG3525-T50B versions antérieures à 5.50(ABPM.7.1)C0
  - EMG5523-T50B versions antérieures à 5.50(ABPM.7.1)C0
  - EX2210-T0 versions antérieures à 5.50(ABPM.7.1)C0
  - EX3300-T0 versions antérieures à 5.50(ABPM.7.1)C0
  - EX3300-T1 versions antérieures à 5.50(ABPM.7.1)C0
- Fiber ONTs :
  - PX3321-T1 versions antérieures à 5.44(ACJB.1.5)C0
  - PX3321-T1 versions antérieures à 5.44(ACHK.3)C0

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- PX5301-T0 versions antérieures à 5.44(ACKB.0.6)C0

- Répéteurs sans fil :
  - WX5610-B0 versions antérieures à 5.18(ACGJ.0.5)C0

Identificateurs externes :

- CVE-2025-11845, CVE-2025-11846, CVE-2025-11847, CVE-2026-1459 ;
- CVE-2025-11848, CVE-2025-13942, CVE-2025-13943 ;

Bilan de la vulnérabilité :

Zyxel a publié un avis de sécurité concernant plusieurs vulnérabilités affectant certains équipements réseau. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant de provoquer un déni de service (DoS), d'exécuter des commandes système non autorisées via des requêtes spécialement conçues (HTTP/CGI ou UPnP) ainsi de compromettre la disponibilité et l'intégrité des équipements concernés.

Solution :

Veuillez se référer au bulletin de sécurité ZyXEL du 24 Février 2026 afin d'installer les nouvelles mises à jour.

Risque :

- Exécution de commandes arbitraires ;
- Atteinte à la confidentialité des données ;
- Atteinte à l'intégrité des données ;
- Déni de service (DoS) ;

Référence :

Bulletin de sécurité ZyXEL du 24 Février 2026:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026