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	Vulnérabilité critique dans pare-feux ZyXEL
Numéro de Référence	51242911/24
Date de Publication	29 Novembre 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Zyxel ATP version V5.00 à V5.38,
- Zyxel version USG FLEX V5.00 à V5.38,
- Zyxel version USG FLEX 50(W) V5.10 à V5.38,
- Zyxel version USG20(W)-VPN V5.10 à V5.38.

Identificateurs externes

- CVE-2024-11667

Bilan de la vulnérabilité

Zyxel annonce la correction d'une vulnérabilité critique exploitée par des acteurs malveillants ciblant les pare-feux Zyxel. Une vulnérabilité de traversée de répertoire dans l'interface de gestion web des versions des pare-feu Zyxel susmentionnées pourrait permettre à un attaquant de télécharger ou d'envoyer des fichiers via des URL falsifiées.

Solution :

Pour se protéger et prévenir d'éventuelles attaques, Zyxel encourage les utilisateurs de prendre les mesures proactives suivantes :

- Mise à jour: mettez immédiatement votre appareil à jour avec la dernière version du micrologiciel.
- Changer les mots de passe administrateur
- Désactivez l'accès à distance : Si les mises à jour ne peuvent pas être appliquées immédiatement, désactivez temporairement l'accès à distance à votre appareil jusqu'à ce que le micrologiciel soit corrigé.

Veuillez se référer au bulletin de sécurité ZyXEL du 27 Novembre 2024 afin d'installer les nouvelles mises à jour.

Risque :

- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données

Référence :

Bulletin de sécurité ZyXEL du 27 Novembre 2024:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-protecting-against-recent-firewall-threats-11-27-2024