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 ZyXEL CPE
Numéro de Référence	52410602/25
Date de Publication	06 Février 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- VMG1312-B10A, VMG1312-B10B, VMG1312-B10E
- VMG3312-B10A, VMG3313-B10A, VMG3926-B10B
- VMG4325-B10A, VMG4380-B10A
- VMG8324-B10A, VMG8924-B10A
- SBG3300, SBG3500

Les modèles VMG1312-B10A, VMG1312-B10B, VMG1312-B10E, VMG3312-B10A, VMG3313-B10A, VMG3926-B10B, VMG4325-B10A, VMG4380-B10A, VMG8324-B10A, VMG8924-B10A, SBG3300 et SBG3500, sont des produits en fin de vie, Zyxel recommande de les remplacer par des équipements de nouvelle génération.

Identificateurs externes

- CVE-2024-40890, CVE-2024-40891, CVE-2025-0890

Bilan de la vulnérabilité

Des failles de sécurité critiques ont été identifiées dans plusieurs dispositifs Zyxel CPE. L'exploitation de ces vulnérabilités permet à un attaquant non authentifié la possibilité d'exécuter du code malveillant et de compromettre entièrement les routeurs vulnérables. Ces vulnérabilités sont actuellement exploitées activement.

Solution :

Veuillez se référer au bulletin de sécurité ZyXEL du 05 Février 2025 afin d'installer les nouvelles mises à jour.

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

Risque :

- Exécution du code arbitraire à distance
- Prise de contrôle du système affecté

Référence :

Bulletin de sécurité ZyXEL du 05 Février 2025:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025