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 critique affectant des firewalls et contrôleurs de point d'accès de Zyxel
Numéro de Référence	28260401/21
Date de publication	04 Janvier 2020
Risque	Critique
Impact	Critique

Systèmes affectés

- ATP series sous firmware ZLD V4.60 antérieure à ZLD V4.60 Patch1
- USG series sous firmware ZLD V4.60 antérieure à ZLD V4.60 Patch1
- USG FLEX series sous firmware ZLD V4.60 antérieure à ZLD V4.60 Patch1
- VPN series sous firmware ZLD V4.60 antérieure à ZLD V4.60 Patch1
- NXC2500 sous firmware V6.00 through V6.10 antérieure à V6.10 Patch1
- NXC5500 sous firmware V6.00 through V6.10 antérieure à V6.10 Patch1

Identificateurs externes

- CVE-2020-29583

Bilan de la vulnérabilité

Zyxel annonce la correction d'une vulnérabilité critique affectant plusieurs versions de ses Firewalls et ses contrôleurs de de point d'accès. L'exploitation de cette vulnérabilité peut permettre à un attaquant de prendre le contrôle de l'équipement vulnérable.

Solution

Veuillez-vous 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

- Prise de contrôle de l’équipement vulnérable.

Référence

Bulletin de sécurité de Zyxel :

- https://www.zyxel.com/support/CVE-2020-29583.shtml