



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans les produits Zyxel Firewall et VPN
<b>Numéro de Référence</b>	42082605/23
<b>Date de Publication</b>	26 Mai 2023
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- ATP version antérieure à ZLD V5.36 Patch 2
- USG FLEX version antérieure à ZLD V5.36 Patch 2
- USG FLEX50(W) / USG20(W)-VPN version antérieure à ZLD V5.36 Patch 2
- VPN version antérieure à ZLD V5.36 Patch 2
- ZyWALL/USG version antérieure à ZLD V4.73 Patch 2

### Identificateurs externes

- CVE-2023-33009, CVE-2023-33010

### Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Zyxel Firewall et VPN. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire à distance et de causer un déni de service.

### Solution :

Veillez se référer au bulletin de sécurité ZyXEL du 06 Septembre 2022 afin d'installer les nouvelles mises à jour.

### Risque :

- Exécution du code arbitraire à distance
- Déni de service

### Référence :

Bulletin de sécurité ZyXEL du 24 Mai 2023 :

- <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls>

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 تدير مركز اليقظة والرصد  
والتصدي للهجمات المعلوماتية، المشور السعيد، ص.ب. 1048 الرباط  
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53  
البريد الإلكتروني contact@macert.gov.ma