



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Zyxel
Numéro de Référence	41600205/23
Date de publication	02 Mai 2023
Risque	Important
Impact	Important

Systemes affectés

- ATP series sous versions de firmware antérieure à ZLD V5.36
- USG FLEX 50(W) / USG20(W)-VPN sous versions de firmware antérieure à ZLD V5.36
- USG FLEX series sous versions de firmware antérieure à ZLD V5.36
- VPN series sous versions de firmware antérieure à ZLD V5.36

Identificateurs externes

- CVE-2023-27990 CVE-2023-27991

Bilan de la vulnérabilité

Zyxel annonce la correction de deux vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'injecter du contenu dans une page ou d'injecter des commandes.

Solution

Veillez-vous référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

Risque

- Injection de contenu dans une page
- Injection de commandes

Référence

Bulletin de sécurité de Zyxel :

- <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-and-post-authentication-command-injection-vulnerability-in-firewalls>