



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans plusieurs produits Zyxel
<b>Numéro de Référence</b>	42260806/23
<b>Date de Publication</b>	08 Juin 2023
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- LTE7480-M804 version antérieure à V1.00(ABRA.7)C0
- LTE7490-M904 version antérieure à V1.00(ABQY.6)C0
- NR7101 version antérieure à V1.00(ABUV.8)C0
- Nebula NR7101 version antérieure à V1.16(ACCC.0)C0
- GS1900-8 version antérieure à V2.70(AAHH.5)
- GS1900-8HP version antérieure à V2.70(AAHL.5)
- GS1900-10HP version antérieure à V2.70(AAZI.5)
- GS1900-16 version antérieure à V2.70(AAHJ.5)
- GS1900-24 version antérieure à V2.70(AAHL.5)
- GS1900-24E version antérieure à V2.70(AAHK.5)
- GS1900-24EP version antérieure à V2.70(ABTO.5)
- GS1900-24HPv2 version antérieure à V2.70(ABTP.5)
- GS1900-48 version antérieure à V2.70(AAHN.5)
- GS1900-48HPv2 version antérieure à V2.70(ABTQ.5)

### Identificateurs externes

- CVE-2022-45853, CVE-2023-27989

### Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Zyxel susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de réussir une élévation de privilèges et de causer un déni de service.

## **Solution :**

Veillez se référer au bulletin de sécurité ZyXEL du 06 Juin 2023 afin d'installer les nouvelles mises à jour.

## **Risque :**

- Elévation de privilèges
- Déni de service

## **Référence :**

Bulletin de sécurité ZyXEL du 06 Juin 2023:

- <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers>
- <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-privilege-escalation-vulnerability-in-gs1900-series-switches>