



BULLETIN DE SECURITE

Titre	Vulnérabilités critique dans les routeurs Netgear
Numéro de Référence	52360502/25
Date de Publication	05 Février 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- WAX206 versions antérieure à 1.0.5.3
- WAX220 versions antérieure à 1.0.3.5
- WAX214v2 versions antérieure à 1.0.2.5

Identificateurs externes

- PSV-2023-0039, PSV-2021-0117

Bilan de la vulnérabilité

Netgear a publié des mises à jour de sécurité pour corriger deux vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de contourner la politique d'authentification afin d'obtenir un accès non autorisé.

Solution

Veillez se référer au bulletin de sécurité Netgear afin d'installer les nouvelles mises à jour.

Risque

- Contourner la politique d'authentification
- Accès non autorisé

Référence

Bulletin de sécurité Netgear du 05 Février 2025:

- <https://kb.netgear.com/000066557/Security-Advisory-for-Authentication-Bypass-on-Some-Wireless-Access-Points-PSV-2024-0117>