



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans plusieurs modèles de routeur Wi-Fi NETGEAR
Numéro de Référence	39613012/22
Date de Publication	30 Décembre 2022
Risque	Critique
Impact	Critique

Systèmes affectés

- RAX40 firmware version antérieure à 1.0.2.60
- RAX35 firmware version antérieure à 1.0.2.60
- R6400v2 firmware version antérieure à 1.0.4.122
- R6700v3 firmware version antérieure à 1.0.4.122
- R6900P firmware version antérieure à 1.3.3.152
- R7000P firmware version antérieure à 1.3.3.152
- R7000 firmware version antérieure à 1.0.11.136
- R7960P firmware version antérieure à 1.4.4.94
- R8000P firmware version antérieure à 1.4.4.94
- RAX75 firmware version antérieure à 1.0.1.64
- RAX80 firmware version antérieure à 1.0.1.64
- R7000 firmware version antérieure à 1.0.11.130
- R7000P firmware version antérieure à 1.3.3.148

Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans plusieurs modèles de routeur Wi-Fi NETGEAR. L'exploitation de cette faille peut permettre à un attaquant d'exécuter du code arbitraire à distance et de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité NETGEAR du 28 Décembre 2022.

Risque

- Déni de service
- Exécution du code arbitraire à distance

Annexe

Bulletins de sécurité NETGEAR du 28 Décembre 2022:

- <https://kb.netgear.com/000065495/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2019-0208>
- <https://kb.netgear.com/000065497/Security-Advisory-for-Denial-of-Service-on-Some-Routers-PSV-2019-0104>