ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilité dans plusieurs produits Netgear
Numéro de Référence	3343221121
Date de Publication	22 Novembre 2021
Risque	Important
Impact	Important

Systèmes affectés

- EX3700 version antérieure à 1.0.0.94
- EX3800 version antérieure à 1.0.0.94
- EX6120 version antérieure à 1.0.0.66
- EX6130 version antérieure à 1.0.0.66
- R6400 version antérieure à 1.0.1.76
- R6400v2 version antérieure à 1.0.4.120
- R6700v3 version antérieure à 1.0.4.120
- R6900P version antérieure à 1.3.3.142_HOTFIX
- R7000 version antérieure à 1.0.11.128
- R7000P version antérieure à 1.3.3.142_HOTFIX
- R7100LG version antérieure à 1.0.0.72
- R7850 version antérieure à 1.0.5.76
- R7900P version antérieure à 1.4.2.84
- R7960P version antérieure à 1.4.2.84
- R8000 version antérieure à 1.0.4.76

- R8000P version antérieure à 1.4.2.84
- R8300 version antérieure à 1.0.2.156
- R8500 version antérieure à 1.0.2.156
- RAX15 version antérieure à 1.0.4.100
- RAX20 version antérieure à 1.0.4.100
- RAX200 version antérieure à 1.0.5.132
- RAX35v2 version antérieure à 1.0.4.100
- RAX38v2 version antérieure à 1.0.4.100
- RAX40v2 version antérieure à 1.0.4.100
- RAX42 version antérieure à 1.0.4.100
- RAX43 version antérieure à 1.0.4.100
- RAX45 version antérieure à 1.0.4.100
- RAX48 version antérieure à 1.0.4.100
- RAX50 version antérieure à 1.0.4.100
- RAX50S version antérieure à 1.0.4.100
- RAX75 version antérieure à 1.0.5.132
- RAX80 version antérieure à 1.0.5.132
- RAXE450 version antérieure à 1.0.8.70
- RAXE500 version antérieure à 1.0.8.70
- RS400 version antérieure à 1.5.1.80
- WNDR3400v3 version antérieure à 1.0.1.42
- WNR3500Lv2 version antérieure à 1.2.0.70
- XR300 version antérieure à 1.0.3.68
- D6220 version antérieure à 1.0.0.76
- D6400 version antérieure à 1.0.0.108

- D7000v2 version antérieure à 1.0.0.76
- DGN2200v4 version antérieure à 1.0.0.126
- DC112A version antérieure à 1.0.0.62
- CAX80 version antérieure à 2.1.3.5

Identificateurs externes

- CVE-2021-34991

Bilan de la vulnérabilité

Une vulnérabilité a été corrigée dans les produits Netgear susmentionnés. L'exploitation de cette faille pourrait permettre à un attaquant d'exécuter du code arbitraire à distance afin de prendre le contrôle du système affecté.

Solution

Veuillez se référer au bulletin de sécurité Netgear du 19 Novembre 2021**.**

Risque

- Exécution de code arbitraire à distance
- Prise de contrôle du système

Annexe

Bulletin de sécurité Netgear du 19 Novembre 2021**:**

- https://kb.netgear.com/000064361/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Multiple-Products-PSV-2021-0168