DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 15-07-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilités affectant des routeurs de Netgear
Réference	1187
Date de Publication	2024-07-15
Sévérité	Elevé

IMPACT :

- Contournement de l'authentification
- Injection de code dans une page
- Exécution de code arbitraire

SYSTÉME AFFECTÉ :

- Netgear CAX30, Firmware avec version antérieure à 2.2.2.2
- Netgear XR1000, Firmware avec version antérieure à 1.0.0.72
- Netgear R7000, Firmware avec version antérieure à 1.0.11.216

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes sur les routeurs susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant de contourner l'authentification, d'exécuter du code arbitraire ou d'injecter du code dans une page.

SOLUTION :

Veuillez se référer au bulletin de sécurité de l'éditeur pour mettre à jour votre produit.

DOCUMENTATION :

Bulletins de sécurité de Netgear :

- https://kb.netgear.com/000066264/Security-Advisory-for-Stored-Cross-Site-Scripting-on-Some-Routers-PSV-2023-0122
- https://kb.netgear.com/000066265/Security-Advisory-for-Authentication-Bypass-on-Some-Cable-Modem-Routers-PSV-2023-0138
- https://kb.netgear.com/000066260/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2023-0079