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	Vulnérabilités critiques dans les routeurs ASUS
Numéro de Référence	47952006/24
Date de Publication	20 Juin 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- ZenWiFi XT8, ZenWiFi XT8 V2
- RT-AX88U, RT-AX58U, RT-AX57
- RT-AC86U, RT-AC68U
- DSL-N12U_C1, DSL-N12U_D1
- DSL-N14U, DSL-N14U_B1
- DSL-N16, DSL-N17U
- DSL-N55U_C1, DSL-N55U_D1
- DSL-N66U, DSL-AC51, DSL-AC750, DSL-AC52U, DSL-AC55U, DSL-AC56U
- DSL-N10_C1, DSL-N10_D1, DSL-N10P_C1 (End-of-life)
- DSL-N12E_C1 (End-of-life)
- DSL-N16P, DSL-N16U (End-of-life)
- DSL-AC52, DSL-AC55 (End-of-life)

Identificateurs externes

- CVE-2024-3912, CVE-2024-3080

Bilan de la vulnérabilité

ASUS a publié des mises à jour de sécurité pour corriger deux vulnérabilités critiques (

CVE-2024-3080 et CVE-2024-3912) dans leurs routeurs. Les vulnérabilités sont les suivantes :

- CVE-2024-3080 : Une vulnérabilité de contournement d'authentification qui peut permettre à un attaquant distant de se connecter à un appareil sans authentification.

- CVE-2024-3912 : Une vulnérabilité qui peut permettre à un attaquant distant non authentifié d'exécuter des commandes système arbitraires sur un appareil.

Solution

Veuillez se référer au bulletin de sécurité ASUS pour plus d'information.

Risque

- Contournement de la politique de sécurité
- Exécution des commandes système arbitraires

Annexe

Bulletins de sécurité ASUS:

- https://www.asus.com/content/asus-product-security-advisory/