ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant des routeurs Asus
Numéro de Référence	43600609/23
Date de publication	06 Septembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- ASUS RT-AX55
- ASUS RT-AX56U_V2
- ASUS RT-AC86U

Identificateurs externes

- CVE-2023-39238 CVE-2023-39239 CVE-2023-39240

Bilan de la vulnérabilité

Asus annonce la correction de trois vulnérabilités critiques affectant ses routeurs susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant disant non authentifié d'exécuter du code arbitraire ou de causer un déni de service.

Solution

Veuillez-vous référer aux bulletins de sécurité d'Asus pour mettre à jours vos équipements.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Déni de service à distance.
- Exécution de code arbitraire

Références

Pages de mise à jour d'Asus :

- https://www.asus.com/networking-iot-servers/wifi-routers/all-series/rt-ax55/helpdesk_bios/?model2Name=RT-AX55
- https://www.asus.com/networking-iot-servers/wifi-routers/asus-wifi-routers/rt-ax56u/helpdesk_bios/?model2Name=RT-AX56U
- https://www.asus.com/supportonly/rt-ac86u/helpdesk_bios/?model2Name=RT-AC86U