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 critique dans Raisecom RAX701-GC
Numéro de Référence	57762410/25
Date de Publication	24 Octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- RAX701-GC-WP-01 (P200R002C52): Firmware version 5.5.27_20190111
- RAX701-GC-WP-01 (P200R002C53): Firmware versions 5.5.13_20180720 et 5.5.36_20190709

Identificateurs externes

- CVE-2025-11534

Bilan de la vulnérabilité

Une vulnérabilité critique de contournement d'authentification a été détectée dans les équipements « Raisecom RAX701-GC », largement déployés dans les environnements industriels et télécoms.

Cette faille permet à un attaquant distant et non authentifié d'obtenir un accès « root » via SSH sans fournir d'identifiants valides, exécuter des commandes système, modifier la configuration, interrompre ou rediriger le trafic, et utiliser l'appareil compromis pour pénétrer d'autres systèmes du réseau.

Solution

Raisecom n'a pas encore annoncée la correction de cette vulnérabilité. Les utilisateurs des produits Raisecom concernés sont invités à contacter le support client Raisecom pour obtenir des informations complémentaires concernant la disponibilité du correctif.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Les mesures suivantes doivent être prises afin de réduire les risques d'exploitation de cette faille :

- Limiter l'exposition réseau de tous les équipements, en s'assurant qu'ils ne soient pas directement accessibles depuis Internet.
- Placer les équipements distants vulnérables derrière des pare-feu, et les cloisonner.
- Utiliser des méthodes d'accès à distance sécurisées, comme un VPN.

Risque

- Elévation de privilèges,
- Exécution des commandes arbitraires,
- Redirection de trafic,

Annexe

Bulletin de sécurité Raisecom du 21 Octobre 2025**:**

- https://www.runzero.com/advisories/raisecom-ssh-bypass-cve-2025-11534/