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 produits Wifi RUCKUS
Numéro de Référence	41911505/23
Date de Publication	15 Mai 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Ruckus E510
- RUCKUS H350 RUCKUS H550 Ruckus H320 Ruckus H500 Ruckus H510
- Ruckus M510 Ruckus M510-JP
- Ruckus P300
- Ruckus Q410 Ruckus Q710 Ruckus Q910
- RUCKUS R350 Ruckus R300 Ruckus R310 Ruckus R320 Ruckus R500 Ruckus R510 Ruckus R550 Ruckus R560 Ruckus R600 Ruckus R610 Ruckus R650 Ruckus R700 Ruckus R710 Ruckus R720 Ruckus R730 Ruckus R750 Ruckus R760 Ruckus R850
- RUCKUS T350d RUCKUS T350se RUCKUS T811-CM (Non-SFP) Ruckus T300 Ruckus T301n Ruckus T301s Ruckus T310c Ruckus T310d Ruckus T310n Ruckus T310s Ruckus T504 Ruckus T610 Ruckus T710 Ruckus T710s Ruckus T750 Ruckus T750SE Ruckus T811-CM SmartZone 100 (SZ-100) SmartZone 144 (SZ-144) SmartZone 144 (SZ-144) - Federal SmartZone 300 (SZ300) SmartZone 300 (SZ300) - Federal ZoneDirector 1000 ZoneDirector 1100 ZoneDirector 1200 ZoneDirector 3000 ZoneDirector 5000

Identificateurs externes

- CVE-2023-25717, CVE-2022-47522

Bilan de la vulnérabilité

Deux vulnérabilités critiques ont été corrigées dans les produits WIFI Ruckus susmentionnés. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire à distance et de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Ruckus**.**

Risque

- Exécution du code arbitraire
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Ruckus**:**

- https://support.ruckuswireless.com/security_bulletins/315
- https://support.ruckuswireless.com/security_bulletins/317