



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant les routeurs TP-Link
Numéro de Référence	57692210/25
Date de Publication	22 Octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- ER8411 version antérieure à 1.3.3 Build 20251013 Rel.44647
- ER7412-M2 version antérieure à 1.1.0 Build 20251015 Rel.63594
- ER707-M2 version antérieure à 1.3.1 Build 20251009 Rel.67687
- ER7206 version antérieure à 2.2.2 Build 20250724 Rel.11109
- ER605 version antérieure à 2.3.1 Build 20251015 Rel.78291
- ER706W version antérieure à 1.2.1 Build 20250821 Rel.80909
- ER706W-4G version antérieure à 1.2.1 Build 20250821 Rel.82492
- ER7212PC version antérieure à 2.1.3 Build 20251016 Rel.82571
- G36 version antérieure à 1.1.4 Build 20251015 Rel.84206
- G611 version antérieure à 1.2.2 Build 20251017 Rel.45512
- FR365 version antérieure à 1.1.10 Build 20250626 Rel.81746
- FR205 version antérieure à 1.0.3 Build 20251016 Rel.61376
- FR307-M2 version antérieure à 1.2.5 Build 20251015 Rel.76743

Identificateurs externes

- CVE-2025-7850, CVE-2025-7851, CVE-2025-6541, CVE-2025-6542

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les routeurs TP-Link susmentionnés. L'exploitation de ces failles peut permettre à un attaquant d'exécuter des commandes arbitraires avec les privilèges de l'administrateur et d'exfiltrer des données sensibles.

Solution

Veuillez se référer au bulletin de sécurité TP-Link du 21 Octobre 2025, afin d'installer les dernières mises à jour.

Risque

- Exécution du code à distance ;
- Exécution des commandes arbitraires ;
- Exfiltration de données sensibles ;

Références

Bulletin de sécurité TP-Link du 21 Octobre 2025:

- <https://support.omadanetworks.com/en/document/108456/>
- <https://support.omadanetworks.com/en/document/108455/>