



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans les routeurs SHARP
<b>Numéro de Référence</b>	51551812/24
<b>Date de Publication</b>	18 Décembre 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- home 5G HR02 versions S5.82.00 et versions antérieures
- Wi-Fi STATION SH-52B versions S3.87.11 et versions antérieures
- Wi-Fi STATION SH-54C versions S6.60.00 et versions antérieures
- Wi-Fi STATION SH-05L versions 01.00.C0 et versions antérieures
- PocketWifi 809SH versions 01.00.B9 et versions antérieures
- Speed Wi-Fi NEXT W07 versions 02.00.48 et versions antérieures

### Identificateurs externes

- CVE-2024-45721 CVE-2024-46873 CVE-2024-47864 CVE-2024-52321 CVE-2024-54082

### Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les routeurs SHARP. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire avec des privilèges « root » ou de compromettre des données sensibles.

### Solution

Veillez se référer au bulletin de sécurité SHARP du 17 Décembre 2024 afin d'installer les nouvelles mises à jour.

### Risque

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données

### Annexe

Bulletins de sécurité JVN du 17 Décembre 2024:

- <https://jvn.jp/en/jp/JVN61635834/index.html>

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](mailto:contact@macert.gov.ma)

المديرية العامة لأمن نظم المعلومات، مديرية تدير مركز اليقظة والرصد  
والتصدي للهجمات المعلوماتية، المشور السعيد، ص.ب. 1048 الرباط  
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53  
البريد الإلكتروني [contact@macert.gov.ma](mailto:contact@macert.gov.ma)