



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 13-09-2026

BULLETIN ALERTES

Object	Vulnérabilité dans MikroTik RouterOS
Référence	1502
Date de Publication	2026-09-05
Sévérité	Critique

IMPACT :

- Contournement de l'authentification SSH
- Usurpation d'un compte utilisateur légitime

SYSTÈME AFFECTÉ :

- MikroTik RouterOS versions **7.24 antérieures à 7.24.2**
- MikroTik RouterOS versions **7.9 antérieures à 7.23.4**

DÉSCRIPTION :

Une vulnérabilité critique a été corrigée dans RouterOS de MikroTik. Elle résulte d'une vérification incomplète de la clé publique RSA lors de l'authentification SSH : le type de clé et le modulus sont contrôlés, mais l'exposant est omis. Un attaquant connaissant le modulus RSA d'un utilisateur autorisé peut fournir une clé forgée avec un exposant fixé à un, produire une signature valide, et ouvrir un canal de commande SSH en usurpant l'identité de cet utilisateur, sans posséder la clé privée correspondante.



SOLUTION :

Mettre à jour MikroTik RouterOS vers l'une des versions corrigées suivantes :

- 7.24.2 ou une version ultérieure
- 7.23.4 ou une version ultérieure

DOCUMENTATION :

Bulletin de sécurité MikroTik :

- <https://mikrotik.com/supportsec/september-2026-vulnerability>

Bulletin de sécurité CERT Polska :

- <https://cert.pl/en/posts/2026/09/mikrotik-routeros-cve/>

CVE-2026-67276 :

- <https://www.cve.org/CVERecord?id=CVE-2026-67276>