

BULLETIN D'ALERTE

N° 0907-BA001

1. INFORMATIONS GÉNÉRALES

Objet	Vulnérabilité critique dans Mikrotik RouterOS
Niveau de criticité	CRITIQUE
Référence	CERT-GN-2026-ALT-001
Date de publication	07 septembre 2026
Niveau de partage	TLP : WHITE

2. RÉSUMÉ

Le RouterOS contient une faille de gestion des arguments dans la connexion SSH, le chemin impliquant des noms d'utilisateur commençant par un caractère interdit, permettant de modifier le masque de politique du RouterOS de confiance, entraînant une escalade de privilèges. L'exploitation nécessite une session SSH non authentifiée pour accéder à l'aide de connexion RouterOS.

Le GN-CERT a découvert que le RouterOS ne compare pas la clé publique **RSA** complète lorsqu'une demande d'authentification **SSH** appartient à une clé utilisateur autorisée, en vérifiant le type de clé et le module de clé mais en omettant l'exposant. Parce que la vérification de signature utilise la clé fournie par le client.

3. RISQUE DE SÉCURITÉ

un attaquant connaissant un module RSA autorisé peut fournir une clé avec l'exposant un, forger une signature valide et ouvrir un canal de commande **SSH** en tant qu'utilisateur cible sans la clé privée. la vulnérabilité peut être activement exploitée avec une combinaison **CVE-2026-67276 + CVE-2026-86060**.

4. CARACTÉRISTIQUES DE LA VULNÉRABILITÉ

Attribut	Valeur
CVE	CVE-2026-67276+ CVE-2026-86060
Score CVSS v3.1	9.8 (Critique)
Versions affectées	(>=) 6.0.0 et avant (<) 6.49.21 ; (>=) 7.0.0 et avant (<) 7.23.4 ; (>=) 7.24 et avant (<) 7.24.2
Version entièrement corrigée	6.49.21 (À long terme), 7.23.4 (À long terme) et 7.24.2 (Stable).

5. RECOMMANDATIONS

Le GN-CERT recommande l'application des mises à jour de sécurité dans les plus brefs délais vers les versions **6.49.21**, **7.23.4** et **7.24.2** de Mikrotik RouterOS.

6. RÉFÉRENCES

<https://cert.pl/en/posts/2026/09/mikrotik-routeros-cve>
<https://forum.mikrotik.com/t/7-23-4-long-term-is-released/272801>
<https://mikrotik.com/supportsec/september-2026-vulnerability/>

