



.....  
Centre de Veille de Détection et de  
Réaction aux Attaques Informatiques

## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant Kubernetes ingress-nginx
<b>Numéro de Référence</b>	60720402/26
<b>Date de Publication</b>	04 février 2026
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systèmes affectés

- ingress-nginx versions antérieures à v1.13.7
- ingress-nginx versions antérieures à v1.14.3

### Identificateur externes

- CVE-2026-1580 CVE-2026-24512 CVE-2026-24513 CVE-2026-24514

### Bilan de la vulnérabilité

Kubernetes annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées de son produit « ingress-nginx ». L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code d'accéder à des données confidentielles ou de causer un déni de service.

### Solution

Veuillez se référer au bulletin de sécurité de l'éditeur pour installer les mises à jour.

## Risque

- Exécution de code
- Accès à des données confidentielles
- Dénier de service

## Références

Bulletin de sécurité de Kubernetes :

- <https://discuss.kubernetes.io/t/security-advisory-multiple-issues-in-ingress-nginx/34115>