



Centre de Veille de Détection et de  
Réaction aux Attaques Informatiques

## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilité critique affectant des produits Zoom
<b>Numéro de Référence</b>	60222101/26
<b>Date de publication</b>	21 janvier 2026
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systèmes affectés

- Zoom Node Meetings Hybrid (ZMH) MMR module versions antérieures à 5.2.1716.0
- Zoom Node Meeting Connector (MC) MMR module versions antérieures à 5.2.1716.0

### Identificateurs externes

- CVE-2026-22844

### Bilan de la vulnérabilité

Zoom annonce la correction d'une vulnérabilité critique affectant ses produits susmentionnés. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code à distance.

### Solution

Veuillez se référer aux bulletins de sécurité de Zoom afin d'installer les nouvelles mises à jour.

### Risque

- Exécution de code à distance

## Référence

Bulletin de sécurité de Zoom:

- <https://www.zoom.com/en/trust/security-bulletin/zsb-26001/>