



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques affectant des Plugins de Jenkins
<b>Numéro de Référence</b>	55551605/25
<b>Date de publication</b>	16 Mai 2025
<b>Risque</b>	Important
<b>Impact</b>	Critique

### Systemes affectés

- OpenID Connect Provider Plugin
- Health Advisor by CloudBees Plugin
- WSO2 Oauth Plugin
- Cadence vManager Plugin
- DingTalk Plugin

### Identificateurs externes

CVE-2025-47884    CVE-2025-47885    CVE-2025-47887    CVE-2025-47886  
CVE-2025-47888    CVE-2025-47889

### Bilan de la vulnérabilité

Jenkins annonce la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. Deux de ces vulnérabilités, identifiées par «CVE-2025-47884» et «CVE-2025-47889» sont critiques et peuvent permettre à un attaquant distant d'injecter du code dans une page, d'accéder à des informations confidentielles ou de contourner des mesures de sécurité.

### Solution

Veillez se référer au bulletin de sécurité de Jenkins pour mettre à jour votre produit.

## Risques

- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Injection de contenu dans une page

## Références

Bulletin de sécurité de Jenkins :

- <https://www.jenkins.io/security/advisory/2025-05-14/>