

The background of the page is a complex network visualization with glowing blue nodes and connecting lines, set against a dark background. Some nodes are labeled with numbers like 5013, 2789, 3659, and 4617.

# Bulletin d'alerte Vulnérabilité critique dans Apache

# Sommaire

<b>CVE-2023-27524</b> .....	<b>2</b>
Type de vulnérabilité .....	2
Risques .....	2
Criticité (score de base CVSS v3.1) .....	2
Produits impactés .....	2
Recommandations .....	3
Preuve de concept .....	3
<b>RÉFÉRENCES</b> .....	<b>4</b>

# CVE-2023-27524

Initialement découverte le 11 octobre 2021, cette vulnérabilité critique de type *Insecure Default Initialization of Ressource* a fait l'objet d'un [bulletin](#) d'alerte par l'éditeur le 24 avril 2023.



L'absence de contrôle du changement du mot de passe par défaut (*SECRET\_KEY*) permet à un attaquant non authentifié et distant, via des requêtes spécifiquement forgées, de contourner les politiques d'accès et d'obtenir des informations sensibles.



Le CISA a intégré cette vulnérabilité dans sa base de données *Known Exploited Vulnerabilities (KEV)* le 08 janvier 2024.

## Type de vulnérabilité

- **CWE-1188** : Insecure Default Initialization of Resource

## Risques

- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données

## Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

## Produits impactés

- Apache Superset versions 2.0.1 et antérieures

## Recommandations

- Mettre à jour Apache Superset vers la version 2.1.0 ou ultérieures.
- Des informations complémentaires sont disponibles dans le [bulletin](#) Apache.

## Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

# Références

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27524>
- <https://lists.apache.org/thread/n0ftx60sllf527j7g11kmt24wvof8xyk>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://www.cisa.gov/news-events/alerts/2024/01/08/cisa-adds-six-known-exploited-vulnerabilities-catalog>