



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans SAP NetWeaver
Numéro de Référence	54172504/25
Date de Publication	25 Avril 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP NetWeaver toutes versions contenant le composant Visual Composer avec MetadataUploader activé.

Identificateurs externes

- CVE-2025-31324

Bilan de la vulnérabilité

Une vulnérabilité critique «CVE-2025-31324» a été découverte dans le composant «MetadataUploader» de «SAP NetWeaver Visual Composer». Cette faille permet à un attaquant distant non authentifié d'uploader et d'exécuter des webshells JSP malveillants, même sur des systèmes à jour. Des attaques actives ont été confirmées.

Solution

- Appliquer immédiatement le correctif officiel fourni par SAP (vérifiez via le SAP Security Patch Day d'avril 2025).
- Restreindre temporairement l'accès au composant MetadataUploader (pare-feu, proxy, ACL).
- Auditer les serveurs SAP exposés sur Internet pour détecter les fichiers Helper.jsp, Cache.jsp ou d'autres uploads suspects ayant les hash suivants :

- **Helper.jsp**
SHA256 :
1f72bd2643995fab4ecf7150b6367fa1b3fab17afd2abed30a98f075e4913087
- **Cache.jsp**
SHA256 :
794cb0a92f51e1387a6b316b8b5ff83d33a51ecf9bf7cc8e88a619ecb64f1dcf

- Activer les journaux d'audit et renforcer les politiques d'authentification sur les composants sensibles.

Risque

- Prise de contrôle du système affecté ;

Référence

Bulletin de sécurité SAP :

- <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html>
- <https://me.sap.com/notes/3594142>