

CVE-2025-31324 : Faille critique activement exploitée sur SAP NetWeaver

Une vulnérabilité critique, référencée CVE-2025-31324, a été découverte dans SAP NetWeaver, plus précisément dans le Visual Composer Développement Server. Pour ainsi dire SAP est un logiciel de gestion intégré centralisant les processus métiers. Ce composant de création d'application optionnel et désactivé par défaut, est activé sur environ 50 % des systèmes SAP Java, ce qui élargit considérablement la surface d'attaque. Comment limiter l'impact d'une vulnérabilité critique sur SAP NetWeaver lorsque celle-ci touche un composant optionnel mais largement utilisé ? La faille permet à un attaquant non authentifié de téléverser et exécuter du code malveillant à distance, compromettant ainsi le serveur ciblé. Avec un score CVSS de 10/10, elle est considérée comme extrêmement critique. Depuis le 27 mars 2025, des groupes malveillants exploitent activement cette vulnérabilité, déposant notamment des fichiers pour prendre le contrôle des systèmes. D'après le moteur de recherche Onyphe, 1 284 serveurs vulnérables sont accessibles en ligne, dont 474 déjà compromis. Plusieurs grandes entreprises françaises et internationales sont concernées, notamment dans les indices CAC 40, SBF 120 et Fortune 500. SAP a publié un correctif le 25 avril 2025, précédé d'une mesure d'atténuation temporaire dès le 8 avril. Le CERT-FR recommande de vérifier si le composant vulnérable est activé (via l'URL système), de rechercher des fichiers suspects dans certains répertoires applicatifs, et d'inspecter les journaux Web pour identifier toute activité anormale. Cette situation démontre que même des composants jugés secondaires peuvent présenter des risques majeurs s'ils sont largement déployés. Il est urgent pour toutes les entreprises concernées d'appliquer les correctifs, de réviser leur architecture, et de renforcer leurs mécanismes de détection pour prévenir de futures compromissions.

Sources

<https://www.it-connect.fr/plus-de-1-200-serveurs-sap-vulnerables-a-une-faille-critique-des-attaques-sont-en-cours/>

<https://www.lemagit.fr/actualites/366623051/SAP-NetWeaver-la-vulnerabilite-critique-qui-menace-les-plus-grand>