AVIS DE SECURITE

Objet	**Multiples vulnérabilités critiques dans les produits SAP (Security Patch Day d'octobre 2026)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-258
TLP	WHITE

Résumé

SAP a publié le 13/10/2026 son Security Patch Day d'octobre 2026, qui corrige plusieurs vulnérabilités dont quatre critiques : exécution de code ABAP injecté dans SAP S/4HANA (CVE-2026-89107, CVSS 9.9), absence de contrôle d'autorisation dans SAP NetWeaver Visual Composer (CVE-2026-89110, CVSS 9.9), élévation de privilèges dans SAP Manufacturing Integration and Intelligence (CVE-2026-89108, CVSS 9.1) et SSRF OAuth2 dans SAP Cloud SDK for Python (CVE-2026-89111, CVSS 10.0). Des vulnérabilités de sévérité élevée affectent également SAP Commerce Cloud (injection SQL, CVSS 8.8), SAP NetWeaver / Web Dispatcher (déni de service non authentifié, CVSS 7.5) et SAP ABAP Platform (CVSS 7.1). Aucune exploitation active n'est signalée à ce jour.

Risque de sécurité

- Exécution de code arbitraire
- Compromission complète du système
- Élévation de privilèges
- Atteinte à la confidentialité des données
- Injection SQL
- Contournement de la politique de sécurité
- Vol d'identifiants OAuth2 (SSRF)
- Déni de service à distance

Systèmes affectés

- SAP S/4HANA (Manage Substitution/Validation Rules) : S4CORE 105, 106, 107, 108 et 109
- SAP NetWeaver Visual Composer : VC70RUNTIME 7.50
- SAP Manufacturing Integration and Intelligence (Configuration Service) : XMII 15.4 et 15.5
- SAP Cloud SDK for Python : versions antérieures à 0.45.2
- SAP Commerce Cloud : COM_CLOUD 2211-JDK21
- SAP NetWeaver et SAP Web Dispatcher (ICM) : KRNL64UC 7.53 ; WEBDISP 7.53, 7.54, 7.77, 7.93, 9.16 ; KERNEL 7.53, 9.18, 9.19, 9.20 ; HDB 2.00 ; XS_ADVANCED_RUNTIME 1.00 ; SAP_EXTENDED_APP_SERVICES 1 ; CONTSERV 7.53
- SAP ABAP Platform (session manager) : KERNEL 7.93 et 9.16

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 13/10/2026 :

- https://url.sap/sapsecuritypatchday
- https://me.sap.com/notes/3805589 (S/4HANA, CVE-2026-89107)
- https://me.sap.com/notes/3797111 (NetWeaver Visual Composer, CVE-2026-89110)
- https://me.sap.com/notes/3798788 (Manufacturing Integration and Intelligence, CVE-2026-89108)
- https://github.com/SAP/cloud-sdk-python/security/advisories/GHSA-4mv3-jxxm-9cx2 (Cloud SDK for Python, CVE-2026-89111)
- https://me.sap.com/notes/3800517 (Commerce Cloud, CVE-2026-89113)
- https://me.sap.com/notes/3765424 (NetWeaver / Web Dispatcher, CVE-2026-58249)
- https://me.sap.com/notes/3626303 (ABAP Platform, CVE-2026-89120)

2. Appliquer les correctifs SAP correspondants en priorité sur les systèmes exposés

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar https://www.stcc-ssi.sn/	E-mail : sncsirt@dcssi.sn	Date de publication : 13/10/2026