AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques dans Adobe Commerce et Magento Open Source (APSB26-138)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-200
TLP	WHITE

Résumé

Le 8 septembre 2026, Adobe a publié sa mise à jour de sécurité mensuelle (APSB26-138) pour Adobe Commerce, Adobe Commerce B2B et Magento Open Source, corrigeant huit vulnérabilités de gravité Critical (CVSS jusqu'à 9.3), principalement des scripts intersites stockés (Stored XSS) et des défauts de contrôle d'autorisation pouvant permettre une élévation de privilèges ou un contournement de fonctionnalité de sécurité. Adobe indique n'avoir connaissance d'aucune exploitation active à ce jour. Cette mise à jour est distincte du correctif d'urgence APSB26-146 du 7 septembre 2026 pour la vulnérabilité « StyleSmuggler » (CVE-2026-75650, déjà couverte par le bulletin SNCSIRT-2026-ADS-191) et doit être appliquée en complément de celui-ci.

Risque de sécurité

- Élévation de privilèges par script intersite stocké (Stored XSS) (CVE-2026-76200, CVSS 9.3, Critical)
- Élévation de privilèges par script intersite stocké (Stored XSS) (CVE-2026-76201, CVSS 9.3, Critical)
- Contournement de fonctionnalité de sécurité par autorisation incorrecte (CVE-2026-77111, CVSS 8.7, Critical)
- Élévation de privilèges par autorisation incorrecte — Adobe Commerce B2B (CVE-2026-77109, CVSS 8.6, Critical)
- Contournement de fonctionnalité de sécurité par autorisation incorrecte (CVE-2026-77774, CVSS 8.6, Critical)
- Élévation de privilèges par autorisation incorrecte (CVE-2026-76202, CVSS 8.2, Critical)
- Contournement de fonctionnalité de sécurité par traversée de répertoire (Path Traversal) (CVE-2026-77110, CVSS 7.6, Critical)
- Élévation de privilèges par autorisation incorrecte — Adobe Commerce B2B (CVE-2026-77108, CVSS 7.5, Critical)

Systèmes affectés

- Adobe Commerce : versions 2.4.9-2026-aug, 2.4.8-2026-aug, 2.4.7-2026-aug, 2.4.6-2026-aug, 2.4.5-2026-aug, 2.4.4-2026-aug et antérieures
- Adobe Commerce B2B : versions 1.5.3-2026-aug, 1.5.2-2026-aug, 1.4.2-2026-aug, 1.3.4-2026-aug, 1.3.3-2026-aug et antérieures
- Magento Open Source : versions 2.4.9-2026-aug, 2.4.8-2026-aug, 2.4.7-2026-aug et antérieures

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 08 septembre 2026 (APSB26-138) :

- https://helpx.adobe.com/security/products/magento/apsb26-138.html
- https://helpx.adobe.com/security/products/magento/apsb26-146.html