AVIS DE SECURITE

Objet	**Multiples vulnérabilités dans Apache Camel (désérialisation non filtrée, injection de code, XXE, contournement d'authentification)**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-273
TLP	WHITE

Résumé

Apache a publié le 19/10/2026 un lot de 38 correctifs de sécurité pour Apache Camel (versions 4.18.5, 4.22.1 et 4.23.0). Plusieurs vulnérabilités permettent l'exécution de code à distance : désérialisation Java non filtrée dans les composants camel-hazelcast (CVE-2026-78162, CVSS v4.0 10.0, code de démonstration public), camel-jgroups (CVE-2026-88900, CVSS v3.1 8.8) et camel-spring-redis (CVE-2026-78165, CVSS v3.1 8.8), ainsi qu'une injection d'expression dans camel-dynamic-router (CVE-2026-83531, CVSS v3.1 8.8).

Aucune exploitation active n'est signalée à ce jour (CVE absentes du catalogue CISA KEV).

Risque de sécurité

- Exécution de code arbitraire à distance
- Atteinte à la confidentialité et à l'intégrité des données
- Contournement de la politique de sécurité (authentification OAuth, contraintes de sécurité Netty-HTTP)
- Injection de requêtes côté serveur (SSRF) et divulgation d'identifiants
- Injection d'entités externes XML (XXE)
- Accès à des fichiers en dehors du répertoire autorisé

Systèmes affectés

- Apache Camel 4.x, versions 4.0.0 antérieures à 4.18.5
- Apache Camel 4.x, versions 4.19.0 antérieures à 4.22.1
- Composant camel-spring-redis : versions depuis 2.11.0 antérieures à 4.18.5 et 4.19.0 à 4.22.1
- Les branches 4.14.x et antérieures sont en fin de vie et ne recevront pas de correctif

Recommandations

Se référer aux bulletins de sécurité de l'éditeur du 19/10/2026 et mettre à jour vers Apache Camel 4.23.0 (ou 4.22.1 / 4.18.5 selon la branche utilisée). En attendant : appliquer un filtre de sérialisation JVM (-Djdk.serialFilter), activer l'authentification et TLS sur les clusters Hazelcast/JGroups :

- https://camel.apache.org/security/
- https://camel.apache.org/security/CVE-2026-78162.html
- https://www.openwall.com/lists/oss-security/2026/10/18/2
- https://nvd.nist.gov/vuln/detail/CVE-2026-78162