AVIS DE SECURITE

Objet	Multiples vulnérabilités importantes dans Apache ZooKeeper
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-212
TLP	WHITE

Résumé

Le projet Apache ZooKeeper a publié le 16 septembre 2026 les versions 3.8.7 et 3.9.6 corrigeant cinq vulnérabilités, dont un contournement d'autorisation sur l'opcode deleteContainer permettant à tout client authentifié de supprimer des znodes sans vérification des ACL (CVE-2026-79993, CVSS 8.1) et un défaut de vérification du nom d'hôte pair en mode quorum TLS/FIPS (CVE-2026-59969, CVSS 7.4). Les autres failles corrigées (injection dans les journaux, divulgation d'informations via rejeu SetWatches) sont de sévérité moindre. Aucune exploitation active n'est signalée.

Risque de sécurité

- Contournement d'autorisation permettant la suppression non contrôlée de znodes (CVE-2026-79993, CVSS 8.1)
- Contournement de la vérification du nom d'hôte pair en quorum TLS/FIPS (CVE-2026-59969, CVSS 7.4)
- Atteinte à la confidentialité des données (divulgation via rejeu SetWatches)
- Contournement de la politique de sécurité (injection dans les journaux d'audit)

Systèmes affectés

- Apache ZooKeeper versions 3.8.x antérieures à 3.8.7
- Apache ZooKeeper versions 3.9.x antérieures à 3.9.6

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 16 septembre 2026 :

- https://zookeeper.apache.org/security.html