



BULLETIN DE SECURITE

| | |
|----------------------------|-------------------------------------|
| Titre | Vulnérabilité dans Apache ZooKeeper |
| Numéro de Référence | 61730903/26 |
| Date de Publication | 09 Mars 2026 |
| Risque | Important |
| Impact | Important |

Systemes affectés

- Apache ZooKeeper version antérieure à 3.9.5 ;
- Apache ZooKeeper version antérieure à 3.8.6 ;

Identificateurs externes

- CVE-2026-24281, CVE-2026-24308 ;

Bilan de la vulnérabilité

Deux vulnérabilités ont été corrigées dans les versions susmentionnées d'Apache ZooKeeper. La première (CVE-2026-24281) est liée à une validation incorrecte du nom d'hôte dans le mécanisme TLS, pouvant permettre une usurpation d'identité et une interception des communications entre les nœuds du cluster. La seconde (CVE-2026-24308) concerne l'enregistrement des informations sensibles dans les fichiers journaux du client, ce qui peut entraîner une divulgation de données sensibles.

Solution

Veillez se référer au bulletin de sécurité d'Apache ZooKeeper du 07 Mars 2026 pour plus d'information.

Risque

- Contournement de la politique de sécurité ;
- Usurpation d'identité ;
- Divulgation d'informations sensibles ;

Annexe

Bulletin de sécurité d'Apache ZooKeeper du 07 Mars 2026:

- <https://lists.apache.org/thread/088ddsbrzhd5lxzbqf5n24yg0mwh9jt2>
- <https://lists.apache.org/thread/qng3rtzv2pqkmko4rhv85jfpklyrgqdr>