



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 13-01-2026

BULLETIN ALERTES

Objet	Vulnérabilité Critique dans Zimbra Collaboration
Référence	1415
Date de Publication	2025-12-22
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance

SYSTÈME AFFECTÉ :

Zimbra versions 10.0.x antérieures à 10.0.18

Zimbra versions 10.1.x antérieures à 10.1.13

DÉSCRIPTION :

Une vulnérabilité de type inclusion de fichiers locaux (Local File Inclusion – LFI) existe dans l'interface Webmail Classic UI de Zimbra Collaboration (ZCS) versions 10.0 et 10.1, en raison d'une mauvaise gestion des paramètres de requête fournis par l'utilisateur dans le servlet RestFilter.

Un attaquant distant non authentifié peut forger des requêtes vers le point d'accès /h/rest afin d'influencer le routage interne des requêtes, ce qui permet l'inclusion de fichiers arbitraires depuis le répertoire WebRoot

SOLUTION :

Mettre à jour Zimbra Collaboration vers la version 10.0.18, 10.1.13 ou ultérieure.
Des informations complémentaires sont disponibles dans le bulletin de Zimbra.

DOCUMENTATION :

- Bulletin de sécurité de ZIMBRA

[Security Center - Zimbra :: Tech Center](#)

- Référence CVE CVE-2025-68645

[CVE Record: CVE-2025-68645](#)