AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Vulnérabilité critique sur les serveurs Zimbra

Contenu

I. Contexte

Des chercheurs en cybersécurité ont mis à jour une vulnérabilité critique de type Cross-Site Scripting (XSS), identifiée sous la référence CVE-2025-48700, qui fait actuellement l'objet d'exploitations actives à grande échelle. Selon eux, plus de 10 500 instances de la suite Zimbra exposées sur internet demeurent vulnérables à cette vulnérabilité.

II. Détails techniques de la vulnérabilité

La faille concerne les versions **ZCS 8.8.15, 9.0, 10.0 et 10.1**. Son exploitation est particulièrement redoutable car elle :

- Ne nécessite aucune interaction de l'utilisateur (Zero-click) ;
- Se déclenche via l'affichage d'un e-mail malveillant dans l'interface Zimbra Classic UI ;
- Permet à un attaquant non authentifié d'exécuter du code JavaScript arbitraire et d'accéder à des données sensibles.

L'attaque peut être entièrement contenue dans le corps HTML d'un e-mail, sans pièce jointe ni lien suspect, rendant sa détection complexe pour les solutions de filtrage traditionnelles.

III. Groupes APT impliqués

Les infrastructures Zimbra sont des cibles privilégiées pour l'espionnage étatique ce qui rend cette situation plus préoccupante. L'agence américaine CISA a récemment ajouté la CVE-2025-48700 à son catalogue d'exploitations connues (KEV Catalog). Bien que les détails spécifiques des attaques actuelles restent confidentiels, le passif de Zimbra illustre l'intérêt des groupes APT.

APT28 (Fancy Bear) a utilisé des failles similaires pour cibler des entités gouvernementales ukrainiennes lors de l'opération GhostMail.

Winter Vivern a exploité des vulnérabilités XSS pour compromettre des portails webmail d'organisations alignées sur l'OTAN.

APT29 (Cozy Bear) a mené des campagnes à "grande échelle" pour dérober des identifiants sur des serveurs vulnérables.

IV. Comment y remédier ?

Face à l'imminence du risque, les administrateurs système doivent agir sans délai pour protéger leurs environnements.

1. Mise à jour immédiate

Il est impératif de mettre à jour les instances vers les dernières versions de maintenance disponibles.

2. Directives de conformité

À l'instar des agences fédérales américaines (FCEB), qui ont reçu l'ordre de sécuriser leurs serveurs sous 72 heures, il est fortement recommandé d'appliquer les correctifs avant le 23 avril.

3. Surveillance accrue

Examiner les journaux d'accès à l'interface Classic UI pour détecter toute activité JavaScript anormale et sensibiliser les utilisateurs à l'importance de signaler tout comportement inhabituel de leur client webmail.

V. Annexes

Les serveurs Zimbra exposés en ligne