CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 12/08/2022

Type de Contenu	Description
Titre	*Vulnérabilités critique dans le service mail Zimbra*
ID	*202208/Alerte/05*
Code LTP	*White*
Niveau de Risque	*Élevé*
Application et service Affectés	*N/A*
Version	*Version inférieure à 8.8.15 p31.1, 9.0.0 p24.1 pour le CVE-2022-27925* *Version inférieure à 8.8.15 p32 et le 9.0.0 P26 Pour le CVE-2022-37042*
Plateforme	*Zimbra*
Mise à jour	*Zimbra version 8.8.15 p33 et 9.0.0 p26*
Résumé	*Vulnérabilité permettant aux attaquants de voler les informations d'identification en clair des utilisateurs des instances Zimbra ciblées*
Impacts	- *Accès au boites mail des victimes* - *Escalade de privilège et avoir accès a d'autre service interne* - *Accès au informations sensible* - *Envoi de messages de phishing aux contacts de l'utilisateur*
Description Détaillée	*La vulnérabilité CVE-2022-27924 est une faille d'injection de commandes dans la plateforme qui pourrait conduire à l'exécution de commandes Menchahed arbitraires et au vol d'information sensibles. Cela est possible en empoisonnant les entrées du cache de la route IMAP dans le serveur Memcached qui est utilisé pour rechercher les utilisateurs Zimbra et transmettre leurs requêtes HTTP aux services dorsaux appropriés. Memcached est un système de stockage clé-valeur en mémoire utilisé comme un cache de haute performance ou un magasin de session pour les bases de données externes et les appels API - dans ce cas, le service de recherche.* *La vulnérabilité CVE-2022-37042 concerne le contournement de l'authentification dans MailBoxImportServlet*

Solutions	*La plateforme Zimbra conseille d'effectuer une mise a jour vers le dernier patch disponible sur leur site si la version en cours d'utilisation est antérieure au version 8.8.15 P33 et 9.0.0 P26*
Liens pour plus de détails	*https://blog.sonarsource.com/zimbra-mail-stealing-clear-text-credentials-via-memcache-injection/*