CYBER DEFENSE AFRICA : ANNONCE SÉCURITÉ **Date** : 04/02/2022

Type de Contenu	Description
Titre	*Zero-day dans la plateforme de messagerie open source Zimbra*
ID	*202202/Alerte/03*
Code LTP	*White*
Niveau de Risque	*Élevé*
Application et service Affectés	*Zimbra 8.8.15 P29 et P30*
Version	*NA*
Plateforme	*NA*
Mise à jour	*Zimbra version 9.0.0*
Résumé	*Vulnérabilité permettant le vol des e-mails*
Impacts	- *Vol des emails* - *Exfiltration de cookies pour permettre un accès persistant à une boîte aux lettres électronique* - *Envoi de messages de phishing aux contacts de l'utilisateur* - *Affichage d'une invitation à télécharger des logiciels malveillants à partir de sites web de confiance*
Description Détaillée	*La vulnérabilité Zero-day découverte a été utilisée dans des campagnes de spear-phishing qui ont débuté en décembre 2021 par un groupe malveillant soupçonné d'être d'origine chinoise. Selon les informations obtenues les campagnes se sont déroulées en plusieurs vagues et en deux phases d'attaque. La phase initiale visait la reconnaissance et comportait des courriels conçus pour vérifier simplement si une cible recevait et ouvrait les messages. La deuxième phase s'est déroulée en plusieurs vagues, avec des messages électroniques incitant les cibles à cliquer sur un lien malveillant créé par l'attaquant. Pour que l'attaque réussisse, la cible devait visiter le lien de l'attaquant tout en étant connectée au client de messagerie Zimbra depuis un navigateur web. Le lien lui-même, cependant, pourrait être lancé à partir d'autre application tel que Thunderbird ou Outlook. Une exploitation réussie permet à l'attaquant d'exécuter un JavaScript arbitraire (cross-site scripting, injection de code) dans le contexte de la session Zimbra de l'utilisateur.*

Solutions	*Les ingénieurs de Zimbra ont vérifié le problème et produit un correctif pour la version 8.8.15 P30. Ce correctif sera disponible pour les clients Zimbra via le support Zimbra. Un correctif durable pour le problème est en cours de test et d'examen de qualité et sera disponible en tant que mise à jour de la version 8.8.15 P30. La disponibilité du correctif mis à jour est prévue via leur site de téléchargement le 5 février 2022.* *Le problème ne concerne que Zimbra 8.8.15 et les versions antérieures. Il est recommandé à tous les clients Zimbra d'utiliser la version (Zimbra version 9.0.0) la plus récente disponible pour éviter tout problème.*
Liens pour plus de détails	*https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/*