CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 18/09/2024

Type de Contenu	Description
Titre	***Correctifs publiés pour des vulnérabilités critiques dans des serveurs vCenter et VMware Cloud Foundation.***
ID	*202409/AS/25*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	***Serveurs vCenter et Produits VMware Cloud Foundation.***
Version / Edition	- *vCenter Server 8.0* - *vCenter Server 7.0* - *VMware Cloud Foundation 5.x* - *VMware Cloud Foundation 4.x*
Plateforme	***vCenter et vmWare Cloud Foundation.***
Mise à jour	- *vCenter Server 8.0 (corrigé dans 8.0 U3b)* - *vCenter Server 7.0 (Corrigé dans 7.0 U3s)* - *VMware Cloud Foundation 5.x (corrigé dans 8.0 U3b)* - *VMware Cloud Foundation 4.x (Corrigé dans 7.0 U3s)*
Résumé	*Publication d'un avis de sécurité critique concernant deux vulnérabilités pour les **serveurs VMware vCenter**.*
Impacts	- ***Exécution du code à distance et escalade de privilèges au niveau root ;*** - ***Prise du contrôle total des systèmes affectés ;*** - ***Modification des configurations de sécurité et Installation de logiciels malveillants;*** - ***Accès et exfiltration de données confidentielles et sensibles.***
Description Détaillée	*VMware a publié un avis de sécurité critique **(VMSA-2024-0019)** concernant deux vulnérabilités importantes dans ses produits vCenter Server et VMware Cloud Foundation. Identifiées sous les noms de **CVE-2024-38812 et CVE-2024-38813,** ces vulnérabilités affectent les serveurs **vCenter (versions 7.0 & 8.0)** et le produit **VMware Cloud Foundation (versions 4.x&5.x).*** *Une exploitation réussie de ces vulnérabilités peut conduire à l'exécution de code à distance, permettant aux attaquants d'élever leurs privilèges au niveau root et de prendre le contrôle des systèmes affectés.* *D'après l'entreprise Broadcom (VMware), « Ces vulnérabilités sont des problèmes de gestion de la mémoire et de corruption qui peuvent être utilisés contre les services VMware vCenter, permettant potentiellement l'exécution de code à distance ». Par contre, elle déclare ne pas avoir connaissance d'une exploitation malveillante des deux vulnérabilités, mais invite ses clients à mettre à jour leurs installations avec les dernières versions afin de se prémunir contre les menaces potentielles.* *VMware a publié des mises à jour pour corriger ces vulnérabilités.*

Recommandations	***VMware conseille vivement à tous les utilisateurs des produits concernés d'appliquer rapidement ces mises à jour afin de réduire les risques potentiels associés à ces vulnérabilités.*** *Ci-dessous les produits/versions affectés et leurs correctifs :* - *vCenter Server 8.0 (corrigé dans 8.0 U3b)* - *vCenter Server 7.0 (Corrigé dans 7.0 U3s)* - *VMware Cloud Foundation 5.x (corrigé dans 8.0 U3b)* - *VMware Cloud Foundation 4.x (Corrigé dans 7.0 U3s)*
Indicateurs de Compromission	*N/A*
Liens pour plus de détails	*https://blogs.vmware.com/cloud-foundation/2024/09/17/vmsa-2024-0019-questions-answers/*

Annexe : *Matrice de réponse concernant les deux vulnérabilités (**CVE-2024-38812 et CVE-2024-38813**)*

VMware Product	Version	CVE(s)	CVSSv3	Severity	Fixed Version
vCenter Server	8.0	CVE-2024-38812, 38813	9.8, 7.5	Critical	8.0 U3b
vCenter Server	7.0	CVE-2024-38812, 38813	9.8, 7.5	Critical	7.0 U3s
VMware Cloud Foundation	5.x	CVE-2024-38812, 38813	9.8, 7.5	Critical	Async patch to 8.0 U3b
VMware Cloud Foundation	4.x	CVE-2024-38812, 38813	9.8, 7.5	Critical	Async patch to 7.0 U3s

Figure 1: Matrice de réponse