CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 07/11/2023

Type de Contenu	Description
Titre	*Nouvelles vulnérabilités CVE découvertes dans 2 produits VMware.*
ID	*202311/AS/20*
Code TLP	*Green*
Niveau de risque	*CVE-2023-34048 : Critique* *CVE-2023-34056 : Medium*
Application et service affectés	• VMware vCenter Server versions 8.x antérieures à 8.OU2 et 8.OU1d • VMware vCenter Server versions 7.x antérieures à 7.OU3o • VMware vCenter Server versions 6.7.x antérieures à 6.7U3 sans le dernier correctif exceptionnel (version en fin de support) • VMware vCenter Server versions 6.5.x antérieures à 6.5U3 sans le dernier correctif exceptionnel (version en fin de support) • VMware Cloud Foundation (VMware vCenter Server) versions 5.x sans le dernier correctif de sécurité (cf. KB88287) • VMware Cloud Foundation (VMware vCenter Server) versions 4.x sans le dernier correctif de sécurité (cf. KB88287) • VMware Cloud Foundation (VMware vCenter Server) versions 3.x sans le dernier correctif de sécurité (cf. KB88287)
Version / Edition	• VMware vCenter Server • VMware Cloud Foundation
Plateforme	***VMware***
Mise à jour	*Mise à jour vers la dernière version disponible.*
Résumé	Deux vulnérabilités de sévérité critique et Medium ont été découvertes dans VMware vCenter Server et VMware Cloud Foundation. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et d'avoir un accès a des données sensibles.
Impacts	***Atteinte à la confidentialité des données.***
Description Détaillée	La vulnérabilité **CVE-2023-34048** de sévérité Critique avec un score CVSSv3 de base maximum de 9.8 affecte vCenter Server. En effet il a été découvert que ce produit de VMware contient une vulnérabilité en écriture hors limites dans l'implémentation du protocole DCERPC. Ainsi un acteur malveillant disposant d'un accès réseau à vCenter Server peut déclencher une écriture hors limites conduisant potentiellement à une exécution de code à distance.

	La vulnérabilité **CVE-2023-34056** affectant le vCenter Server est une vulnérabilité de type divulgation partielle d'information. Cette vulnérabilité a été évalué comme étant dans la gamme de gravité Medium avec un score CVSSv3 de base maximum de 4.3. Un acteur malveillant disposant de privilèges non administratifs sur vCenter Server peut exploiter cette faille pour accéder à des données non autorisées.
Solutions	*Appliquer les dernières mises à jour fournit par VMware en fonction du produits concernés.*
Liens pour plus de détails	• *https://www.cve.org/CVERecord?id=CVE-2023-34048* • *https://www.cve.org/CVERecord?id=CVE-2023-34056* • *https://documentation.stormshield.eu/SNS/v4/fr/Content/User_Configuration_Manual_SNS_v4/Protocols/MS_RPC_Protocol.htm* • *https://www.vmware.com/security/advisories/VMSA-2023-0023.html*