CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 30/07/2024

Type de Contenu	Description
Titre	***Exploitation de la vulnérabilité Zerologon (CVE-2020-1472) par le groupe cybercriminel « Ransomhub » pour faire des victimes dans ses récentes attaques.***
ID	*202407/AS/09*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	***Windows Server version 2004, 2016, 2019, 1903, 1909*** ***Windows Server 2008 R2 Service Pack*** ***Windows Server 2012, R2*** ***Windows Server version 20H2***
Version / Edition	*A partir des versions 10.0.0*
Plateforme	***Systèmes basés sur x64***
Mise à jour	*Microsoft avait publié début août 2020, les patchs qui corrigent cette vulnérabilité dans tous les systèmes affectés par la vulnérabilité CVE-2020-1472*
Résumé	*Exploitation de la vulnérabilité Zerologon (CVE-2020-1472) dans les récentes attaques du groupe cybercriminel Ransomhub*
Impacts	- ***Exécution des attaques de commandes ou d'injection SQL programmées*** - ***Exfiltration, violation et divulgation des données importantes et sensibles des victimes*** - ***Chiffrement de données et blocage des systèmes*** - ***Pertes financières énormes***
Description Détaillée	*Le groupe cybercriminel « RansomHub » a utilisé la vulnérabilité Zerologon (CVE-2020-1472) pour obtenir les privilèges d'administrateur de domaine et faire plusieurs victimes dans ses récentes attaques. Il a déjà publié les données de plusieurs de ses victimes tout en exigeant la rançon à d'autres.* *RansomHub est un important groupe de ransomware qui fonctionne selon le modèle* ***« Ransomware-as-a-Service »*** *(RaaS). Ce groupe fournit à ses affiliés des outils et une infrastructure de ransomware prêts à l'emploi, facilitant ainsi les attaques sophistiquées de ransomware sans expertise technique particulière.* *La vulnérabilité CVE-2020-1472 du protocole Netlogon, alias Zerologon, permet aux cybercriminels de pirater les contrôleurs de domaine et mener leurs attaques. Une vulnérabilité de type élévation de privilèges existe lorsqu'un attaquant établit une connexion de canal sécurisé Netlogon vulnérable avec un contrôleur de domaine, en utilisant le protocole à distance Netlogon (MS-NRPC).*
Recommandations	***Microsoft a publié début août 2020, les patchs qui corrigent cette vulnérabilité dans tous les systèmes affectés par la vulnérabilité CVE-2020-1472. A cet effet, il faut :*** • ***Vérifier et mettre à jour urgemment vos contrôleurs de domaine avec une***

	mise à jour ultérieure à celle publiée par Microsoft depuis le 11 août 2020. • ***Mettre régulièrement à jour les systèmes afin d'empêcher l'exploitation des vulnérabilités connues telles que Zerologon.*** • ***Effectuer des sauvegardes régulières.*** • ***Vérifier via une EDR, l'absence des indications de Compromission (IOCs) dans vos systèmes.***
Indicateurs de Compromission	*Hashs SHA 256 :* - *02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292* - *104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2* - *2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad* - *34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087* - *36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e* - *595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb* - *7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2* - *7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a* - *8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7* - *a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2* - *e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23* - *ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00* - *f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3* - *fb9f9734d7966d6bc15cce5150abb63aadd4223924800f0b90dc07a311fb0a7e*
Liens pour plus de détails	*https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472* *https://www.linkedin.com/feed/update/urn:li:activity:7223988477091057664* */?updateEntityUrn=urn%3Ali%3Afs_updateV2%3A%28urn%3Ali%3Aactivity* *%3A7223988477091057664%2CFEED_DETAIL%2CEMPTY%2CDEFAULT%2Cfalse%29*