ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	Un nouveau Ransomware-as-a-Service "MichaelKors" cible VMware ESXi
Numéro de Référence	41941705/23
Date de Publication	17 Mai 2023
Risque	Critique
Impact	Critique

Des nouvelles compagnes d'attaques ciblent activement les systèmes VMware ESXi dans le monde entier à l'aide de nouveaux ransomwares. En effet, un nouveau programme ransomware-as-a-service (RaaS) nommé "MichaelKors" a été identifié qui fournit aux affiliés des binaires de ransomware capables de cibler les environnements ESXi.

Les acteurs de la menace pourraient accéder directement à VMware par le biais d'un vol d'informations d'identification, ou à l'interface d'administration d'ESXi. Une fois l'accès obtenu, les acteurs de la menace pouvaient utiliser les informations d'identification volées pour authentifier le serveur VMware et modifier le compte d'utilisateur local afin d'obtenir un accès privilégié. Ils pouvaient ainsi exécuter des commandes arbitraires et accéder à la console Secure Shell (SSH). Dans le cas où un compte compromis fournit un accès administratif à un environnement de machine virtuelle (VM), les acteurs de la menace pourraient reconfigurer la VM en tant que proxy pour accéder au réseau interne.

Il est fortement recommandé d'interdire l'accès direct aux hôtes ESXi, activer l'authentification multifactorielle (MFA) pour tous les comptes, sauvegarder régulièrement les volumes ESXi et appliquer les correctifs de sécurité, afin de minimiser l'impact des attaques de l'hyperviseur.

Annexe

- https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma