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	BlackByte Ransomware exploite VMware ESXi vulnérabilité
Numéro de Référence	49090309/24
Date de Publication	09 septembre 2024
Risque	Critique
Impact	Critique

Le groupe de ransomware BlackByte exploite activement la vulnérabilité « CVE-2024-37085 » de contournement d'authentification récemment corrigée dans les hyperviseurs VMware ESXi pour déployer des ransomwares et obtenir un accès administratif complet aux réseaux des victimes.

Le maCERT recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT en cas de détection d'une activité relative à ce malware.

Indicateurs de compromission (IOCs):

Hashs :

- 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd
- 0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5
- 31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427
- 543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91

Annexe :

- https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/

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