



## NOTE DE SECURITE

|                            |                                                         |
|----------------------------|---------------------------------------------------------|
| <b>Titre</b>               | BlackByte Ransomware exploite VMware ESXi vulnérabilité |
| <b>Numéro de Référence</b> | 49090309/24                                             |
| <b>Date de Publication</b> | 09 septembre 2024                                       |
| <b>Risque</b>              | Critique                                                |
| <b>Impact</b>              | 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/>