Clef de chiffrement stockée en dur : VMware aussi

VMware vient de sortir en urgence un patch pour vSphere Data Protection (VDP), une appliance virtuelle s'intégrant à vCenter et fournissant une gestion centralisée des sauvegardes (jusqu'à 100 VM). En cause : une clef SSH codée en dur qui permet potentiellement à un assaillant de s'emparer d'un accès root sur cette technologie.

Dans l'article publié sur son site de support, VMware reconnaît que son appliance VDP contient une clef privée SSH statique, que l'éditeur présente comme « *compromise* ». Sans toutefois préciser si cette compromission se traduit par des attaques réelles sur le terrain. Cette clef, autorisée par défaut sur VDP, permet qui plus est une interopérabilité avec les technologies de déduplication d'EMC Avamar.

Une seconde faille dans ESXi

« *Un assaillant ayant un accès au réseau interne pourrait exploiter cet accès à l'appliance avec des privilèges root pour parvenir à une compromission totale du système* », écrit le spécialiste de la virtualisation dans son alerte. VMware classe cette faille comme critique. Et recommande l'application du patch pour les versions 5.5 à 6.1 de vSphere Data Protection.

La présence d'accès codés en dur demeure une faille de sécurité très courante, malgré les efforts de l'industrie pour abolir cette pratique. Rappelons que la constitution des botnets Mirai, capables de lancer des attaques DDoS à la puissance inégalée, repose précisément sur l'infection d'appareils ayant des codes d'accès statiques, stockés dans leur microcontrôleur.

En parallèle du patch pour cette faille critique, VMware corrige une seconde vulnérabilité touchant l'hyperviseur ESXi. Ce défaut, de type cross-site scripting, permet une attaque contre ESXi à partir d'une VM spécialement configurée par un assaillant. VMware, qui juge cette faille importante, livre un correctif pour les versions 5.5 et 6.0 de son produit.

A lire aussi :

Conteneurs : pourquoi VMware adopte Kubernetes

AWS + VMware : un accord qui peut changer la face du Cloud

Crédit Photo : SergeyNivens-Shutterstock