

Rapport de Sécurité

Administration Système et Réseaux

Azzouz Souhaïb | VAN DEN SCHRIECK Virginie | 29/09/2019

La liste des risques encourus par votre VPS et votre infrastructure Docker :

OVH met à notre disposition des machines dont la responsabilité nous revient. En effet, n’ayant aucun accès à ces machines, OVH n’en est pas les administrateurs. Si le VPS n’est pas sécurisé il peut se faire attaquer sur Internet.

Les contre-mesures mises en place

* Mettre à jour le système
* Modifier le port d’écoute par défaut du service SSH
* Modifier le mot de passe associé à l’utilisateur “root”
* Désactiver l’accès au serveur via l’utilisateur root
* Installer et configurer le paquet Fail2ban
* Authentification par clef

Risques encourus par chacun des services déployés :

* Service WEB : Les serveurs web peuvent toujours faire l’objet d’attaque que ce soit par des virus ou par des pirates experts. Les conséquences sont constituées généralement par des fuites d’informations personnelles et par l’exploitation des données personnels de l’utilisateur.
* Service DNS : il existe des virus qui modifient les paramètres réseaux pour diriger les requêtes DNS vers des serveurs pirates, il pourrait y avoir des fuites d’informations qui sont personnelles à l’utilisateur.
* Service VoiP : Une destruction des données ou introduction de contenus pirates, , un déni de service qui submerge le serveur VoiP de spams.

Les contre-mesures mises en place

Service web : Activation des certificats SSL

Annexes