***Fortnite : Les joueurs risquent gros, VulnÃ©rabilitÃ© des donnÃ©es.***
**Internet**
PostÃ© par : JulieM
PubliÃ©e le : 17/1/2019 13:00:00

Les chercheurs de Check PointÂ® Software Technologies Ltd., l'un des principaux fournisseurs de solutions de cybersÃ©curitÃ© dans le monde, dÃ©voilent dans le dÃ©tail les vulnÃ©rabilitÃ©s qui auraient pu affecter les joueurs du fameux jeu de combat en ligne Fortnite.

Fortnite compte prÃ¨s de 80 millions de joueurs dans le monde. TrÃ¨s populaire, le jeu tourne sur toutes les plateformes, depuis Android, iOS ou PC via Microsoft Windows jusquâ□□aux consoles Xbox One et PlayStation 4.




En plus des joueurs occasionnels, Fortnite est utilisÃ© par les joueurs professionnels qui utilisent leurs sessions en ligne et il rencontre un franc succÃ¨s auprÃ¨s des amateurs de sports Ã©lectroniques.

Si elle avait Ã©tÃ© dÃ©couverte, la faille aurait donnÃ© aux pirates un accÃ¨s total au compte utilisateur et informations personnelles dâ□□un joueur lambda.Â

Elle aurait Ã©galement permis lâ□□accÃ¨s Ã  lâ□□option de paiement par monnaie virtuelle proposÃ©e dans le jeu, et lâ□□utilisation frauduleuse de sa carte de paiement.

GrÃ¢ce Ã  cette faille un pirate aurait pu Ã©couter les conversations dans le jeu ainsi que les bruits environnants Ã©manent du domicile de la victime ou tout autre endroit dÃ©diÃ© au jeu, portant ainsi atteinte Ã  sa privÃ©e.

Sachant que des joueurs de Fortnite ont Ã©tÃ© rÃ©cemment la cible dâ□□escroqueries les incitant Ã  se connecter Ã  de faux sites Web contre la promesse de gÃ©nÃ©rer de la monnaie de jeu 'V-Buck' de Fortnite, ces nouvelles failles auraient pu Ãªtre exploitÃ©es, sans mÃªme que le joueur ait Ã  fournir les informations de connexion.

Les experts de Check Point ont rÃ©ussi Ã  dÃ©crypter le processus de piratage dâ□□un compte utilisateur Fortnite au travers de failles dans le processus de connexion au jeu, rÃ©vÃ©lant ainsi trois niveaux de vulnÃ©rabilitÃ©s dans l'infrastructure Web d'Epic Games, plus particuliÃ¨rement dans le processus d'authentification par jeton utilisÃ© avec les systÃ¨mes de Single Sign-On (SSO) via Facebook, Google et Xbox.

Elles auraient permis de voler les informations d'accÃ¨s des utilisateurs et prendre contrÃ´le de leur compte.

ConcrÃ¨tement, un joueur n'avait qu'Ã  cliquer sur un lien d'hameÃ§onnage artisanal provenant Ã  premiÃ¨re vue dâ□□Epic Games et permettant la capture du jeton d'authentification Fortnite de l'utilisateur par le pirate au moyen de deux sous-domaines vulnÃ©rables identifiÃ©s dans le jeu par les experts Check Point, et ce, sans que l'utilisateur n'ait Ã  rentrer ses identifiants de connexion.

Â« Fortnite est l'un des jeux les plus populaires du moment, notamment auprÃ¨s des enfants. Ces failles auraient pu porter atteinte Ã  leur vie privÃ©e et celle de leur famille de maniÃ¨re significative Â», explique Oded Vanunu, responsable de la recherche sur la vulnÃ©rabilitÃ© des produits chez Check Point.

Â« Avec les failles que nous avons rÃ©cemment recensÃ©es dans les plates-formes utilisÃ©es par le fabricant de drones DJI, on voit Ã  quel point les applications cloud sont vulnÃ©rables aux attaques.

Ces plates-formes sont de plus en plus ciblÃ©es par les pirates informatiques en raison de l'Ã©norme quantitÃ© de donnÃ©es sensibles qu'elles contiennent. L'authentification Ã  double facteur pourrait attÃ©nuer cette vulnÃ©rabilitÃ© de prise de contrÃ´le de comptes par des pirates. Â»

Check Point a alertÃ© Epic Games de la vulnÃ©rabilitÃ©, laquelle est dÃ©sormais corrigÃ©e. Check Point et Epic Games conseillent Ã  tous les utilisateurs de rester vigilants lorsqu'ils Ã©changent des informations par voie numÃ©rique, et d'adopter des habitudes cybernÃ©tiques sÃ»res lorsqu'ils interagissent en ligne.Â

Ensemble, ils attirent Ã©galement lâ□□attention sur le fait que les utilisateurs doivent aussi se mÃ©fier des liens vers des informations disponibles sur les forums d'utilisateurs et les sites Web.

Les entreprises doivent effectuer des contrÃ´les rÃ©guliers et approfondis de leur infrastructure informatique et vÃ©rifier qu'elles n'ont pas laissÃ© des sites ou des points d'accÃ¨s obsolÃ¨tes et inutilisÃ©s accessibles en ligne. En outre, il est recommandÃ© d'examiner tout site Web ou domaines obsolÃ¨tes encore accessibles en ligne mais pas utilisÃ©s.

Afin de rÃ©duire les menaces, les utilisateurs doivent activer l'authentification Ã  double facteur, en s'assurant dâ□□entrer un code de sÃ©curitÃ© envoyÃ© aux adresses e-mail du titulaire du compte lorsqu'ils se connectent Ã  leur compte depuis un nouveau pÃ©riphÃ©rique.Â

Il est Ã©galement important que les parents sensibilisent leurs enfants Ã  la menace de fraude en ligne et les avertissent du fait que les cybercriminels feront tout pour avoir accÃ¨s Ã  leurs donnÃ©es personnelles et financiÃ¨res.

***Pour une analyse dÃ©taillÃ©e des vulnÃ©rabilitÃ©s Fortnite :***