CyberArk : VulnÃ©rabilitÃ© dans Windows Hello.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 15/7/2021 13:00:00

Le Labs de CyberArk a publiÃ© de nouvelles recherches relatives Ã une vulnÃ©rabilitÃ© importante identifiÃ©e dans Windows Hello, qui permet Ã un attaquant de contourner l'authentification par reconnaissance faciale sur l'appareil dâ□□un utilisateur cible.Â

La vulnÃ©rabilitÃ© a reÃ§u un CVE (score) et a Ã©tÃ© corrigÃ©e aujourd'hui dans la version Patch Tuesday de Microsoft.

Le Labs de CyberArk est l'Ã©quipe de recherche ayant dÃ©couvert la technique sophistiquÃ©e GoldenSAML que les attaquants de SolarWinds ont utilisÃ©e afin de perpÃ©trer l'une des attaques de supply chain les plus Ã©laborÃ©es jamais rÃ©alisÃ©es.Â

Selon cette nouvelle recherche, cette preuve de concept sur la faÃ§on de contourner la reconnaissance faciale pour l'authentification pourrait avoir un impact similaire sur les campagnes d'espionnage ciblÃ©es Ã travers le monde.

Selon Microsoft, 85 % des utilisateurs de Windows 10 utilisent Windows Hello pour l'authentification sans mot de passe.Â

L'Ã©quipe de recherche de CyberArk a trouvÃ© un moyen de manipuler les aspects de sÃ©curitÃ© derriÃ¨re le mÃ©canisme de reconnaissance faciale utilisÃ© par Windows Hello, via une camÃ©ra USB sur mesure et une photo de lâ□□utilisateur cible.

Si l'objectif des chercheurs Ã©tait Windows Hello, il ressort que le POC a des implications pour tout systÃ¨me d'authentification permettant Ã une camÃ©ra USB tierce enfichable de servir de capteur biomÃ©trique.

Comme le montre la recherche, ce type d'attaque est trÃ¨s pertinent pour l'espionnage ciblÃ©, lorsque la cible est connue et qu'un accÃ¨s physique est nÃ©cessaire sur un appareil.Â

Il sâ□□agirait dâ□□une attaque trÃ¨s efficace contre un chercheur, un scientifique, un journaliste, un militant ou toute autre personne avec une adresse IP sur son appareil.

A ce sujet, Omer Tsarfati, chercheur en sÃ©curitÃ©, au sein du Labs de CyberArk et auteur de cette recherche commente :

Â« Nos tests prÃ©liminaires nous ont permis de constater que l'utilisation dâ□□une connexion sÃ©curisÃ©e renforcÃ©e par du matÃ©riel compatible limite la surface d'attaque mais dÃ©pend des utilisateurs ayant des camÃ©ras spÃ©cifiques.Â

Parce quâ□□elle est inhÃ©rente Ã la conception du systÃ¨me, la confiance par dÃ©faut des accÃ¨s des pÃ©riphÃ©riques reste. Pour attÃ©nuer ce problÃ¨me de confiance inhÃ©rent de maniÃ¨re plus complÃ¨te, l'hÃ´te doit donc valider l'intÃ©gritÃ© du dispositif d'authentification biomÃ©trique avant dâ□□accorder sa confiance. Â».

Plus d'info. (VO)