Windows à lui aussi droit à sa faille ShellShock

The Security Factory met aujourd'hui en lumière une faille permettant à un utilisateur Windows de lancer une commande en mode administrateur. Une vulnérabilité assez proche de la faille Shellshock découverte sur les systèmes Unix utilisant Bash, et aisée à exploiter.

Il suffit en effet de créer un dossier dont le nom se termine par le caractère '&' suivi de la commande que vous souhaitez lancer. Cette dernière sera alors exécutée avec les droits administrateur par le script vulnérable présent sur la machine.

Reste bien évidemment à trouver un tel script sur le serveur. La condition requise pour que cette vulnérabilité soit exploitable est que la variable d'environnement %CD% (qui pointe sur le nom du répertoire courant) soit utilisée au sein du script. Chose assez courante sur les serveurs de fichiers.

Microsoft ne proposera pas de correctif

Alerté, Microsoft indique ne pas souhaiter corriger ce problème, qui n'est pas une faille de sécurité, mais une mauvaise utilisation des variables d'environnement. La firme recommande ici d'utiliser « %CD% » et non %CD% afin de se prémunir de ce problème.

Ce changement permet en effet d'éviter l'exploitation de cette vulnérabilité. *The Security Factory* indique toutefois avoir trouvé sans peine des scripts exploitant la variable %CD% sans guillemets, et invite donc les administrateurs système à auditer leurs serveurs de fichiers Windows.

Sur le même thème

Yahoo confirme, puis dément, avoir été piraté via la faille Shellshock
Faille Shell Shock : la Free Software Foundation réagit promptement
Bugzilla : une faille zero day révèle les bugs des logiciels

Crédit photo : © Pavel Ignatov – Shutterstock