BadTunnel : la faille qui touche tous les Windows depuis 20 ans

Un chercheur en sécurité chinois a découvert une vulnérabilité grave, baptisée BadTunnel, dans toutes les versions du système d'exploitation Windows, de Windows 95 à Windows 10. Ce qui signifie que cela fait désormais plus de 20 ans que les utilisateurs sont exposés à ce risque.

Microsoft a livré, lors de son dernier Patch Tuesday, une rustine pour cette faille (lire le bulletin de sécurité MS16-077), ce qui a permis à Yang Yu, le fondateur du Xuanwu Lab de Tencent, de révéler quelques détails de BadTunnel dans un entretien avec nos confrères de Dark Reading. Yu aurait gagné la plus haute récompense du bug bounty de Microsoft, soit 50 000 dollars.

« *Cette vulnérabilité a un impact considérable – probablement le plus important de l'histoire de Windows*, explique Yang Yu. BadTunnel peut non seulement être exploité à travers de nombreux canaux différents, mais il existe aussi dans toutes les versions de Windows des 20 dernières années. La faille peut être exploitée en toute discrétion avec un taux de réussite proche de 100 %. » Même si rien n'indique, à ce jour, qu'elle l'ait réellement été.

BadTunnel détourne le trafic

BadTunnel cache une technique d'usurpation d'identité sur les réseaux (NetBIOS-spoofing), profitant d'une erreur de codage au sein de Windows. Il permet à l'assaillant d'accéder au trafic du réseau de sa victime sans en être un utilisateur légitime. L'attaque contourne également le pare-feu et les services de Network Address Translation (NAT).

« *Cette vulnérabilité est causée par une série d'implémentations en apparence correctes, qui comprennent un protocole de couche de transport, un protocole de couche applicative, quelques usages spécifiques de ce dernier par l'OS et plusieurs implémentations de protocoles utilisées par les pare-feu et des services NAT* », précise Yu.

Pour compromettre sa victime, l'attaquant doit la pousser à visiter une page web piégée avec Edge ou Internet Explorer. Ou l'infecter via un dispositif de stockage vérolé ou un document Office truqué. Le site de l'attaquant apparaît alors comme un serveur de fichiers ou un serveur d'impression local, en mesure de détourner le trafic réseau de sa victime (HTTP, Windows Update, et même les mises à jour de la liste des certificats révoqués via Microsoft CryptoAPI).

Réflexions dans un avion

Essentiellement, BadTunnel exploite une série de faiblesses de sécurité, y compris la façon dont Windows résout les noms de réseau et accepte les réponses. C'est l'addition de tous ces défauts qui rend l'attaque BadTunnel possible.

Yu aurait commencé à mettre au jour cette faille lors d'un déplacement en avion, l'année dernière. Il a commencé à imaginer de nouveaux scénarios d'attaque avant de tester la théorie échafaudée

en vol sur différentes configurations. Ce qui l'a amené à détecter la faille Windows. Une trouvaille dont il a informé Microsoft en janvier dernier.

A lire aussi :

Windows 10 Anniversary Update : Microsoft lance la chasse aux bugs

Patch Tuesday : IE, Edge, Windows Server et Office colmatés

Une pétition contre les migrations forcées vers Windows 10

Crédit photo : wk1003mike / Shutterstock