Faille critique sur le service ‘Wins’ de Windows

‘Wins’ permet la résolution de noms Netbios en adresses IP sur un réseau local. Il est généralement utilisé lorsque plusieurs domaines cohabitent ou lorsque l’administrateur veut se passer des « broadcasts » sur son réseau. Une faille critique vient d’être découverte dans ce service. Elle a été mise à jour par un spécialiste, Nicolas Waisman, un responsable de la société Immunity.

L’exploitation de la faille pourrait permettre l’exécution de code arbitraire à distance (sur le LAN). Pour le moment aucun correctif n’est disponible mais des contres–mesures existent. Une fois de plus, l’exploitation de la faille pourrait être triviale. Il suffirait d’envoyer un paquet mal formé sur le serveur Wins vulnérable pour perturber gravement le fonctionnement de la machine. L’exécution de code arbitraire serait possible. La faille affecte, entre autres cibles: – Windows 2000 Server (SP2 à SP4), – Windows 2003 Server – Windows NT4 Server. Pour se prémunir d’une éventuelle attaque, le filtrage du port 42 en « tcp & udp » est de mise. L’utilisation d’IPSec pour sécuriser le trafic entre serveurs WINS réplicants est également une solution en attendant un correctif de Microsoft. Pour les plus radicaux, il est recommandé de désactiver Wins temporairement. D’après l’auteur de cette alerte, sa découverte remonterait à Mai 2004. Comment expliquer un tel décalage entre cette date et l’annonce publique par Immunity? Cette société est à la tête d’un club « privé » dédié à l’échange de vulnérabilités et d’exploits baptisé l’ « Immunity Vulnerability Sharing Club ». Le principe est simple : confiner les bonnes infos dans ce cercle d’amis très fermé. Le ticket d’entrée à ce club V.I.P est de 50.000 dollars US. Qui a dit que le business des exploits n’existait pas ?… L’alerte Nicolas Waisman http://www.immunitysec.com/downloads/instantanea.pdf