Une faille critique frapperait les VPN IPSec

IPSec est un ensemble de protocoles développés par l'IETF qui a pour vocation d'établir des canaux de communication sécurisés garantissant l'intégrité et la confidentialité des données véhiculées via le protocole IP (

Internet protocol). IPSec est largement utilisé par les équipements VPN en entreprise. Certaines configurations IPSec qui utilisent notamment l'ESP (*Encapsulating security payload*) ou AH (*Authentication header*) seraient vulnérables à une attaque permettant d'intercepter les données en clair. **Un dogme s'effondre** La confidentialité des données véhiculées ainsi à travers un tunnel IPSec est donc remise en question. Un dogme s'effondre. D'après le NISCC, cette vulnérabilité (CAN-2005-0039) a pu être démontrée en laboratoire au prix d'un effort *« modéré »*. Bien sûr, l'attaque requiert que l'assaillant puisse intercepter les paquets IPSec sur le réseau. Dans son bulletin d'alerte, le NISCC offre plusieurs préconisations afin de « fixer » temporairement la vulnérabilité en attendant un correctif de la part des éditeurs concernés par la faille. Le NISCC recommande notamment aux utilisateurs de solutions IPSec d'utiliser l'ESP en activant et en combinant la protection de confidentialité ainsi que la protection d'intégrité. L'émission de messages d'erreurs devrait également être désactivée ou filtrée (ICMP) au niveau du 'firewall'. (*) **pour Vulnerabilite.com**