OpenSSL et les produits Cisco sont durement attaqués

La vulnérabilité découverte dans OpenSSL permet de faire tomber à l'aide d'une requête malformée les produits qui exploitent l'outil libre.

L'attaque a lieu au moment de l'initialisation d'une connexion sécurisée SSL/TLS (la fameuse « poignée de main » chère au protocole TCP). OpenSSL étant très utilisé, notamment aux côtés du serveur web Libre Apache, cette faille concerne potentiellement de très nombreux systèmes. Et parmi ces derniers, nombreux sont ceux embarqués au sein de boîtiers matériels : le couple Apache / OpenSSL offre en effet une solution d'administration web sécurisée idéale pour les constructeurs de matériel, et, surtout, gratuite. Cisco est le premier fabriquant à avoir reconnu être touché par cette faille, et à publier les correctifs nécessaires. La société utilise OpenSSL dans de nombreux produits, dont certains pare-feux PIX, des routeurs de la gamme 7000 et Catalyst, ainsi que des 'switches' de la gamme MDS et plusieurs autres applications. Une liste complète est disponible sur le site de l'éditeur. En ce qui concerne OpenSSL lui-même, deux nouvelles versions sont disponibles, qui corrigent la vulnérabilité (0.9.7d et 0.9.6m). L'alerte chez OpenSSL (en Anglais). http://www.openssl.org/news/secadv_20040317.txt Source: « Les Nouvelles.net » agence d'information dédiée à la sécurité informatique.