Cyberespionnage : RSA et NSA main dans la main ?

Reuters dévoile aujourd'hui que la NSA aurait signé un contrat de 10 millions de dollars avec le spécialiste de la sécurité RSA (aujourd'hui filiale d'EMC), afin que ce dernier **affaiblisse ses algorithmes de sécurité**.

L'objectif était de favoriser la diffusion de logiciels de chiffrement que l'agence de sécurité américaine soit en mesure de pirater aisément.

Les documents divulgués par **Edward Snowden** expliquent que RSA aurait adopté un algorithme piégé de création de nombres aléatoires. Grâce à ce dernier, les chiffres générés n'auraient rien de non prédictible, ce qui mettrait à mal le niveau de sécurité des offres de chiffrement l'utilisant. Or, RSA aurait employé cet algorithme dans ses **librairies de cryptographie BSafe**, indique *Reuters*.

RSA dément…

La réponse de l'éditeur ne s'est pas fait attendre. RSA admet avoir travaillé avec la NSA, mais **dans le but de renforcer ses solutions de sécurité**, et non de les affaiblir. Aucune porte dérobée n'aurait donc été installée à la demande de la NSA.

L'algorithme en question n'aurait été utilisé que lorsqu'il recevait l'aval du NIST (National Institute of Standards and Technology). Il a été retiré des offres de RSA depuis que le NIST a recommandé de ne plus l'employer. Recommandation qui est par ailleurs arrivée assez tardivement, puisqu'elle n'a été émise qu'en septembre dernier, alors que les suspicions de l'existence d'une porte dérobée au sein de cet algorithme datent de 2006. RSA avait alors émis un avertissement à destination des clients de BSafe, leur expliquant que cet algorithme, utilisé par défaut au sein du kit de développement du produit, pouvait être poreux aux écoutes de la NSA. L'éditeur s'était toutefois gardé de préciser ses liens financiers avec l'agence de renseignement.

Crédit photo : © John Lee – Fotolia.com

Voir aussi

Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales