Vulnérabilité décelée dans le système de chiffrement d'Office

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 24 janvier 2005

Spyworld Actu

Le module de chiffrement de Word et Excel présente une grave faille : il utilise la même clé pour protéger deux versions d'un fichier. Un non-sens, selon les experts. Microsoft planche sur le problème et pourrait fournir une mise à jour.

Une faille de sécurité importante a été décelée dans le système de chiffrement de Microsoft Office. Elle pourrait être exploitée pour accéder à des documents confidentiels créés avec Word ou Excel, et pourtant protégés par l'utilisateur.

Ces deux applications disposent d'une option "Protéger un document" : quand elle est activée, l'accès au document peut alors être bloqué par un mot de passe et les données sont chiffrées via l'algorithme RC4, avec une clé de 128 bits.

Or Microsoft aurait mal implémenté cette fonction, assure Hongjun Wu, l'expert en cryptographie qui a découvert cette faille. Il travaille au centre de recherche singapourien "Institute of Infocomm Research".

« La conséquence est désastreuse, car une grande quantité d'informations contenues dans le document peut être récupérée facilement », indique-t-il dans son alerte de sécurité. « Quand un document est chiffré [avec Word ou Excel] puis modifié et sauvé, la même clé générée par RC4 est utilisée pour les différentes versions du document », précise-t-il.

Rappelons qu'en matière de chiffrement, une clé générée aléatoirement est utilisée une seule fois pour une meilleure sécurité du message chiffré. Employer une même clé pour plusieurs messages est considéré comme une faille, car il devient alors possible de comparer les données d'un fichier à un autre. Cela permet ainsi de retrouver plus rapidement la clé ayant servi à les protéger.

Une erreur « de niveau maternelle »

Contacté par CNET News.com, Microsoft dit avoir débuté son enquête sur la faille, et précise qu'il fournira le cas échéant une mise à jour. L'éditeur tient cependant à relativiser la portée de cette vulnérabilité devant la probabilité faible du scénario présenté par Hongjun Wu. « L'attaquant doit avoir accès à deux documents distincts ayant le même nom et protégés par le même mot de passe pour exploiter cette vulnérabilité », précise Microsoft.

Une appréciation de la situation qui semble plutôt optimiste. « C'est une erreur de chiffrement de niveau maternelle », n'hésite pas à lancer Bruce Schneier, spécialiste de la cryptographie et responsable technique de la société américaine Counterpane Internet Security. Sur son blog, l'expert déplore que Microsoft n'ait pas retenu ses erreurs passées, rappelant qu'en 1999, une faille équivalente avait été décelée au niveau du chiffrement des mots de passe de Windows NT.

Avec Christophe Guillemin à Paris, pour ZDNet France