Microsoft publie le service pack 3 pour Office 2003

Microsoft vient de publier le troisième « service pack » pour Office 2003. Disponible en téléchargement (140 Mo), ce « service pack » comprend d'importantes mises à jour de sécurité et de stabilité. Il corrige plus de 250 problèmes de performance allant des écrans tremblotants aux plantages d'application sous Access, Excel, InfoPath, Outlook, PowerPoint et Word.

Mais la mise à jour a avant tout porté sur toute une série de problèmes de sécurité, avec quatorze bulletins de sécurité pour Office 2003 qui corrigent chacun plusieurs vulnérabilités dans un seul produit donné.

Ce nouvel accent sur la sécurité résulté d'un profond changement de l'environnement de sécurité, selon David LeBlanc, ingénieur en développement logiciel chez Microsoft. Dans une note publiée sur un blog du groupe, il met ce changement sur le compte d'une hausse du nombre de programmes malveillants commerciaux et sur la valeur accrue des vulnérabilités utilisées pour installer du code malveillant.

« Lorsque nous avons publié Office 2003, nous étions fiers de notre travail et pensions que ce produit était parfaitement sûr », ajoute-t-il. *« Tout s'est très bien passé durant les deux premières années qui ont suivi sa commercialisation. Puis les pirates ont commencé à changer de tactiques et nous avons commencé à rencontrer de nombreux problèmes. »*

Lorsque les pirates ont commencé à recourir à de nouvelles tactiques, les vulnérabilités d'Office ont commencé à s'accumuler et la suite est devenue une cible de choix pour les exploits. *« Nous avons fait un très bon travail avec Office 2003 pour combattre les techniques d'attaque qui étaient en vigueur en 2003 »*, ajoute l'ingénieur. *« Mais il s'est avéré par la suite qu'il a moins bien résisté aux techniques utilisées en 2006. »*

Microsoft a dû modifier ses propres tactiques pour se mettre au niveau des pirates. Selon David LeBlanc, les développeurs ont beaucoup exploité une technique de test connue sous le nom de « fuzzing » pendant le développement d'Office 2007 et d'Office 2003 SP3.

Cette technique consiste à envoyer de gros paquets de données vers chaque élément d'une application qui gère la saisie de données. Si le logiciel n'est pas suffisamment protégé, le code « fuzz » entraîne son plantage.

La technique est particulièrement répandue car elle permet de détecter facilement des vulnérabilités qui sont souvent exploitées pour installer des logiciels malveillants à distance.

Les développeurs de Microsoft ont commencé à recourir massivement à cette technique pour le développement d'Office 2007. Une fois la suite commercialisée, l'équipe a reproduit cette technique sur Office 2003.

« Nous avons soumis Office 2003 au même niveau d'attaque par fuzzing que celui d'Office 2007 », précise David LeBlanc.

Selon lui, les nouvelles techniques ont été *« redoutables d'efficacité »* pour réduire les menaces, précisant toutefois que, comme l'a appris l'éditeur en 2006, le paysage de la sécurité est en perpétuelle évolution.