Six failles pour IBM Lotus Notes

Six : c'est le nombre de vulnérabilités découvertes au sein de l'outil de communication d'entreprise « IBM Lotus Notes » par les chercheurs de la société danoise Secunia.

Certaines failles permettent de contourner des mécanismes de protection. D'autres offrent, à un éventuel pirate, la possibilité d'exécuter du code arbitraire sur le poste de l'utilisateur. Les failles localisées dans les liens dynamiques DLL kvarcve.dll, tarrdr.dll, udrdr.dll et htmsr.dll permettent, en jouant avec la longueur des noms de fichiers et des URL ?http' et ?ftp' pour la dernière librairie, de déclencher un débordement de mémoire tampon afin d'exécuter les instructions de son choix sur la machine de la victime en bénéficiant des droits de l'utilisateur courant. Une autre vulnérabilité, également localisée dans la DLL kvarcve.dll, pourrait être exploitée afin d'effacer un fichier accessible à l'insu de l'utilisateur de Lotus Notes lors de la prévisualisation d'un fichier compressé aux formats ZIP, UUE ou TAR. Pour finir, une vulnérabilité affectant le composant « HTML Speed Reader » permet également d'exécuter du code arbitraire lorsqu'un utilisateur visualise une page HTML piégée. Ces problèmes de sécurité sont confirmés pour les versions 6.5.4 à 7.0 de Lotus Notes. D'après les experts, les versions antérieures sont probablement tout autant vulnérables. Réactivité oblige, IBM met à disposition deux mises à jour, les versions 6.5.5 et 7.0.1 qui corrigent les lacunes découvertes.