Les derniers patchs Microsoft comblent bien des failles made in NSA

Les correctifs de sécurité que Microsoft vient de publier pour des OS que l'éditeur ne supportent plus – Windows XP et Windows Server 2003 en particulier – corrigent bien des failles mises au jour à l'occasion de la divulgation des outils de hacking de la NSA.C'est la seconde fois que Redmond se voit obligé de corriger des vulnérabilités lâchées dans la nature par les fuites de données dont a été victime l'agence de renseignement de Fort Meade. La première fois, des hackers avaient exploité une faille Windows dans le protocole SMB pour accélérer la diffusion d'un ransomware, le tristement célèbre WannaCry. Créant une crise mondial. Ce qui avait poussé Microsoft à patcher le trou de SMB y compris sur des versions d'OS qu'il ne supportait plus (à commencer par XP).

Cette fois, le premier éditeur mondial, anticipant un « *risque élevé de cyberattaques destructrices* », a décidé de prendre les devants. Dans son alerte, la société américain évoque une « *potentielle activité d'un Etat* » autour de ces failles, sans toutefois mentionner ni la nation en question, ni l'origine de ses soupçons. L'éditeur précise que la publication de patchs pour des OS non supportés restera exceptionnelle et ne doit pas être « *interprétée comme une modification des règles standards* ».

Patcher ? Difficile sur certains systèmes métier

Rappelons qu'un groupe de hackers inconnu jusqu'en août dernier, les Shadow Brokers, a obtenu l'accès à un ensemble d'outils de hacking de la NSA, outillage permettant à l'agence américaine de pénétrer des systèmes Windows, Linux ou Solaris, des équipements réseau ou des firewalls. Ces outils d'exploitation de failles jusqu'alors inconnues ont été dévoilés peu à peu par les Shadow Brokers (après les vains efforts de ces derniers pour les monnayer au prix fort). La divulgation des exploits made in NSA a poussé Microsoft à patcher ses systèmes supportés en avril dernier, laissant de côté trois outils de hacking qui ne ciblaient que des OS ne bénéficiant plus de mises à jour de la part de Redmond. Ce sont ces trois exploits – appelés EnglishManDentist, EsteeMaudit et ExplodingCan – que Microsoft vient contrarier avec la sortie de ses derniers correctifs pour Windows XP et Server 2003. Si ces deux systèmes sont effectivement totalement obsolètes, ils animent encore un grand nombre de systèmes, rendant les attaques utilisant les 3 exploits de la NSA à la fois dangereuses et assez simples à mettre en œuvre.

Le fait de disposer de correctifs, y compris pour des systèmes vieillissants, est évidemment positif pour les organisations qui continuent à les exploiter. Mais ne règle qu'une partie du problème créé par la divulgation des exploits de la NSA. Car Windows XP, notamment, est souvent embarqué dans des systèmes métier spécifiques, qu'il est très difficile de mettre à jour en raison des risques d'instabilité que l'application des patchs fait peser. Comme l'a montré WannaCry dont les dégâts les plus significatifs se sont manifestés sur des systèmes industriels (Renault en France). « *Cette fameuse informatique industrielle connectée au SI traditionnel, mais n'évoluant pas au même rythme, pose de gros soucis* », reconnaissait récemment Alain Bouillé, le RSSI de la Caisse des dépôts et président du Cesin, un club de RSSI.

A lire aussi :

Microsoft patche une nouvelle fois Windows XP et Server 2003

Thales : « les systèmes les plus critiques sont aussi les plus vulnérables à WannaCry »

WannaCry : le ransomware qui n'a plus besoin du phishing

Crédit Photo : produktionsbuero TINUS-Shutterstock