Certificats vulnérables : Microsoft vient au secours de Dell

Microsoft vient donner un coup de main à Dell, ou plutôt aux utilisateurs des PC du constructeur texan qui hébergent des certificats vulnérables. eDellRoot et DSDTestProvider ont été découverts par des utilisateurs ces derniers jours. Si Dell assurent que ces certificats ne visent pas à espionner les données des utilisateurs comme a pu le faire Lenovo avec Superfish, les logiciels n'en constituent pas moins des menaces de sécurité de par les vulnérabilités qu'ils présentent.

Pour eDellRoot, Dell a fourni mode d'emploi et un outil pour éradiquer la présence du certificat. Mais les utilisateurs peu enclins à mettre la main à la pâte (ou pas informés de ces problématiques) pourront aussi compter sur la vigilance de Microsoft. L'éditeur de Windows annonce avoir mis à jour ses solutions de sécurité en conséquence.

Windows 10 à Vista sécurisés

Plusieurs outils peuvent détecter et supprimer le certificat de Dell identifié comme Win32/CompromisedCert.D. L'anti malware Windows Defender pour Windows 10 et 8.1, et l'anti-virus Microsoft Security Essentials pour Windows 7 et Vista. Pour les férus de manipulations, s'y ajoutent l'analyseur Microsoft Safety Scanner et l'outil de suppression manuel Microsoft Software Removal Tool.

Autant d'outils disponibles gratuitement qui visent à protéger les clients de Dell et, donc indirectement, ceux de Redmond (qui, au passage, met ses outils de sécurité en avant). Microsoft rappelle que Win32/CompromisedCert.D (ou eDellRoot) est un certificat racine propre à Dell pour lesquels les clés privées ont été divulguées en ligne. Exploité à des fins malintentionnées, le certificat vulnérable permet à un attaquant de signer des logiciels et sites pour faire croire au système qu'ils sont légitimes et accorder potentiellement le contrôle total de la machine à distance ou de la navigation en ligne afin de voler des informations confidentielles (identifiants de comptes en ligne, données personnelles…). Les attaquants doivent néanmoins user de techniques de phishing ou d'attaques par l'homme-du-milieu (man-in-the-middle) pour installer des malware, modifier ou usurper des adresses Internet en HTTPS. Une barrière supplémentaire qui ne doit rien enlever à la vigilance de l'utilisateur.

Lire également
Certificat de sécurité expiré = chaos sur Mac App Store
HTTPS : Google menace de blacklister les certificats de Symantec
Les certificats SSL contrefaits étudiés à la loupe

Crédit Photo : SergeyNivens-Shutterstock