Microsoft XP + SP3, contrer les failles Zero-Day de l' USB
Microsoft
PostÃ© par : JulieM
PubliÃ©e le : 22/7/2010 0:00:00

Vendredi dernier, Microsoft a publiÃ© lâ□□alerte de sÃ©curitÃ© 2286198, confirmant que toutes les versions supportÃ©es de Windows contiennent une faille critique. Cette nouvelle vulnÃ©rabilitÃ© zero-day sâ□□exploite facilement via les dispositifs USB, le partage rÃ©seau ou les partages WebDAV distants. Pour que cette faille soit exploitable, il suffit simplement de visionner les contenus du dispositif USB dans Windows Explorer.

Des raccourcis spÃ©cialement crÃ©Ã©s (.lnk) autorisent lâ□□exÃ©cution du code au moment oÃ¹ lâ□□icÃ´ne du raccourci se charge dans lâ□□interface graphique. Les exploits sâ□□appuyant sur cette faille sont limitÃ©s pour le moment mais sont trÃ¨s certainement amenÃ©s Ã se multiplier dans les semaines Ã venir.

Cette vulnÃ©rabilitÃ© â□□shortcutâ□□ a Ã©tÃ© dÃ©couverte lors dâ□□une analyse du rootkit Stuxnt, qui avait servi pour des attaques ciblant les systÃ¨mes SCADA de la sociÃ©tÃ© Siemens. Ces systÃ¨mes aident surtout Ã la supervision et Ã lâ□□acquisition de donnÃ©es dans les environnements industriels, comme les centrales Ã©lectriques. Le dossier Â« shortcut Â» utilisÃ© dans ce cas de figure a Ã©tÃ© dÃ©tectÃ© sous le nom : **Exploit W32/WormLink.A**.

La situation est dÃ©sormais plus dÃ©licate. La semaine derniÃ¨re, une version Â« proof of concept Â» disponible au public a Ã©tÃ© transmise Ã plusieurs sites hÃ©bergeant des bases de donnÃ©es dâ□□exploit. Le code correspondant Ã cet exploit Â« proof of concept Â» est maintenant dans la nature, et F-Secure sâ□□attend Ã ce que les crÃ©ateurs de virus sâ□□approprient cette mÃ©thode dâ□□attaques dans les prochaines semaines.

Sean Sullivan, Security Advisor chez F-Secure, explique : Â« *Ce ver reprÃ©sente un vÃ©ritable danger. La situation risque dâ□□empirer jusquâ□□Ã la publication dâ□□un correctif de la part de Microsoft. De plus, le Service Pack 2 pour Microsoft XP nâ□□Ã©tant plus supportÃ©, mÃªme le correctif risque de ne pas pouvoir rÃ©soudre totalement le problÃ¨me. Les enquÃªtes menÃ©es par*

F-Secure montrent en effet que de nombreuses entreprises continuent dâ□□utiliser le Service Pack 2. Â»

F-Secure conseille vivement aux entreprises de migrer au plus vite vers le Service Pack 3 de Windows XP ou dâ□□appliquer les suggestions de Microsoft pour solutionner le problÃ¨me.

ParallÃ¨lement, les entreprises doivent absolument crÃ©er ou mettre Ã jour les rÃ¨gles de sÃ©curitÃ© concernant les dispositifs USB. Â« *Le danger que reprÃ©sente cette faille peut Ãªtre attÃ©nuÃ© en observant de Â« bonnes pratiques Â». Une entreprise nâ□□incluant pas les dispositifs USB dans les rÃ¨gles de sÃ©curitÃ© se met par dÃ©finition en danger. Celle qui, en revanche, a mis en place des politiques, devra les rÃ©Ã©tudier afin de sâ□□assurer quâ□□elles sont correctement appliquÃ©es. Cette dÃ©marche doit Ãªtre rapidement mise en Å□uvre Ã lâ□□approche des vacances dâ□□Ã©tÃ©* Â» continue **Sean Sullivan**.