

[Faille : des clés USB ouvrent les portes de Windows...](#)

Il est loin le temps où une disquette avec « ntfs2dos » et « pwdump2 » suffisait pour récupérer en local la base SAM d'une station Windows NT4 afin de voler les droits administrateurs de la machine. Les nouvelles technologies affluent et remplacent les systèmes désuets. Les clés USB remplacent les lecteurs de disquette, mais de nouvelles failles apparaissent.

Ainsi, la société SPI Dynamics annonce la découverte d'une vulnérabilité affectant les pilotes (drivers) USB pour les systèmes d'exploitation Microsoft Windows 32-bit incluant Windows 2000 et Windows XP. La faille, de type « buffer overflow », permettrait de prendre la main en local sur une station verrouillée et d'obtenir les droits administrateur. Pour exploiter la vulnérabilité, il suffit d'un programme spécifique déposé sur une clé USB que l'on branche sur la station Windows verrouillée dont on veut prendre instantanément le contrôle. Caleb Sima, CTO de Spi Dynamics, explique que Microsoft n'a pas été avisé de la découverte et qu'une démonstration en sera faite cette semaine lors des BlackHat Briefings à Las Vegas. Pour le moment, la société Spi Dynamics a décidé de ne livrer que peu d'informations techniques concernant ce défaut de sécurité. Affaire à suivre.

Aurélien Cabezon pour [Vulnerabilite.com](#)