

Windows: un fallo en la memoria USB

20/07/2010 10:07 by Canarios

Windows: un fallo en las claves USB Microsoft publicados en este momento un boletín de seguridad de un nuevo fallo que afecta a varias versiones de Windows, incluyendo XP SP3, Vista SP1, SP2, e incluso Windows 7 beta.

La compañía de windows dice que esta vulnerabilidad es causada "por un análisis insuficiente de los accesos directos, lo que puede provocar la ejecución de código malicioso cuando el usuario hace clic en un icono de acceso directo a la modificación. Este error es especialmente utilizado por un malware llamado Stunxnet inicial previamente identificados por el equipo de seguridad VirusBlokAda. Este rootkit también funciona en modo de ejecución automática: sólo tiene que enchufar una memoria USB infectada, y abrir el contenido con el Explorador de Windows (o cualquier otra utilidad) para generar el ataque.

Pantalla de Windows 7

El ataque se caracteriza por la inserción de un archivo. Dll archivos ocultos en dos mrxnet.sys y mrxcls.sys. Este último habría obtenido un certificado de Verisign para validar el RealTek fabricante. Esto permite la introducción de código en los procesos del sistema. Microsoft afirma que si el usuario está conectado como las disposiciones administrativas del sistema, podría tomar el control de la ordenador para instalar el software, ver, cambiar o eliminar datos o crear la cuenta de administrador otros.

Por esta razón, un usuario inicia sesión como invitado en su ordenador sólo se consideraba menos vulnerables. F-Secure expertos agregaron que el rootkit es capaz de propagarse a otros medios de comunicación conectado a USB, sino también en el almacenamiento de red conectada a través de WebDAV el servicio WebClient en Windows. se recomienda el cierre del servicio y desactivar visualización de los iconos para los accesos directos. No sabemos si Microsoft lanzará un parche de corrección antes de su próxima programada para el Martes, 10 de agosto 2010 próximo.