Asociación de Internautas

Graves vulnerabilidades en Windows

Ejecución de código mediante un archivo de imagen (.BMP, .CUR, .ICO, .ANI)

La vulnerabilidad afecta a los Windows NT/2K/XP SP0-SP1/2K3 y es del tipo "integer oberflow", afecta a la función API LoadImage perteneciente a la biblioteca USER32.DLL. Dicha vulnerabilidad existe debido a un mal tratamiento del tamaño atribuido a la imagen en su propia cabecera.

Un atacante podría modificar el código de la cabecera de uno de los tipos de imágenes afectadas, es decir, de un cursor (.cur, .ani), un icono (.ico) o una imagen bitmap (.bmp) e integrarla en una web o en un correo electrónico de forma que al ser vista por la víctima el código malicioso incluido en la cabecera de la imagen se ejecutaría en el sistema de la víctima de forma silenciosa.

Post en Bugtraq:
(http://www.securityfocus.com/archive/1/385342)

El autor ha publicado una demostración que abre el puerto 28876 al ser abierta con el Internet Explorer 6 (http://www.xfocus.net/flashsky/icoExp/loadimage.htm)

-- Fallos en el tratamiento de los archivos .ANI

Los cursores animados utilizados por Windows se guardan en archivos de imagen bajo la extensión.ani. Estos archivos están formados por varias imágenes que se van mostrando sucesivamente, es precisamente la parte de código en la que se detalla la situación de estas imágenes la que es susceptible de ser modificada para crear un ataque.
La vulnerabilidad afecta a los Windows NT/2K/XP SP0-SP1/2K3.

Un atacante podría incluir en una web o un mail un archivo de este tipo especialmente modificado y provocar que el sistema de la víctima se congele o se caiga al ver dicha imagen.

En realidad se trata de 2 vulnerabilidades distintas, porque dependiendo de cómo se manipule la cabecera del archivo, el sistema "víctima" se caerá o se congelará (DOS).

Mas información

Demostración de "crash" (necesita ser abierto con Internet Explorer 6)

Demostración de "DOS" del sistema (necesita ser abierto con Internet Explorer 6)

Fuente: Cyruxnet.org

VI CAMPAÑA DE SEGURIDAD EN LA RED