



HISPASEC SISTEMAS

SEGURIDAD Y TECNOLOGÍAS
DE LA INFORMACIÓN

**Documento técnico:
Múltiples vulnerabilidades en IrfanView 2.4**

Enero 2009

Matthew "j00ru" Jurczyk
matthew@hispasec.com

1. Introducción

IrfanView es un visor de archivos de imagen gratuito y ampliamente extendido para sistemas operativos Windows. Viene provisto de soporte para un gran número de formatos de archivo distintos, incluyendo TIFF (Tagged Image File Format).

Se han descubierto múltiples vulnerabilidades en aplicación que podrían ser aprovechadas por un atacante remoto para causar una denegación de servicio y, potencialmente, lograr la ejecución de código arbitrario.

El problema está causado por un desbordamiento de búfer basado en heap que podría ser aprovechado por un atacante remoto para causar una denegación de servicio en la aplicación, o incluso ejecutar código arbitrario, si un usuario intenta visualizar un archivo de imagen especialmente manipulado.

2. Detalles

Esta sección muestra el análisis detallado de la porción de código vulnerable al desbordamiento de búfer basado en heap:

```
.text:00411CA6      mov     ecx, edi
.text:00411CA8      imul   ecx, [esp+104h+var_CC]
.text:00411CAD      test   ecx, ecx
.text:00411CAF      mov     [esp+104h+var_9C], ecx
.text:00411CB3      jbe    short loc_411CFB
.text:00411CB5      mov     eax, ecx
.text:00411CB7      xor     edx, edx
.text:00411CB9      div    [esp+104h+var_CC]
.text:00411CBD      cmp    eax, edi
.text:00411CBF      jnb    short loc_411CFB
.text:00411CC1      lea    eax, [ecx+ebx*4+28h]
.text:00411CC5      push   eax                ; dwBytes
.text:00411CC6      push   40h                ; uFlags
.text:00411CC8      call   ds:GlobalAlloc
```

Dicha porción de código es responsable de la reserva de un búfer de memoria del tamaño necesario para alojar los datos de la imagen. Antes de la llamada a GlobalAlloc, se calcula el número de bytes necesarios para almacenar de forma segura la totalidad de los datos. Cuando el valor se presenta finalmente en el registro ECX (dirección de memoria 0411CAD) es chequeado otra vez para evitar un posible ataque de desbordamiento de enteros.

```
.text:00411CB9      div    [esp+104h+var_CC]
.text:00411CBD      cmp    eax, edi
.text:00411CBF      jnb    short loc_411CFB
```

Como comprobación se realiza una simple división usando el valor multiplicado, para asegurarse de que $(A*B)/B$ siga siendo A, condición que no se cumpliría en el caso de que la expresión $(A*B)$ causase un desbordamiento. A priori parece una medida bastante razonable, exceptuando un pequeño detalle:

```
.text:00411CC1      lea    eax, [ecx+ebx*4+28h]
```

Antes de realizar la reserva, se añade la constante 28h (40d) al resultado del cálculo y no se realiza la comprobación de un posible desbordamiento de enteros inmediatamente después. La idea es encontrar valores de altura y anchura que no causen el desbordamiento en un primer momento, pero sí una vez se le añade el valor 28h al resultado de su multiplicación. A continuación se muestran una serie de posibles parejas a modo de ejemplo.

21846 65532

24553 58308

24939 57404

24940 57404

25914 55245

26215 54610

26216 54610

... Y más ...

Existen al menos 53 parejas de valores anchura/altura que podrían ser usadas para causar un desbordamiento de búfer basado en heap si se incluyen en un archivo malicioso, posibilitando la ejecución de código arbitrario con los permisos del usuario ejecutando IrfanView.

3. Denegación de servicio al procesar archivos TIFF

IrfanView falla al sanear de forma adecuada ciertos valores introducidos por un usuario en los archivos TIFF. A continuación se detallan varios ejemplos:

- ColorMap tag: desplazamiento de la paleta de imágenes.
Situada en el offset 320 (hex 0x0140).
- Strip Offset tag: uno o más de los valores de 32bits apuntando a una franja en particular de los datos de la imagen.
Situada en el offset 273 (hex 0x0111).
- First Image File Directory offset: un valor DWORD apuntando a la primera estructura IFD.

Estableciendo estos valores a 0xFFFFFFFF (-1) por ejemplo, es muy posible que se generase una excepción del tipo Access Violation al intentar leer en direcciones de memoria no mapeadas, situadas antes de los datos del archivo. Esto podría causar que la aplicación dejase de responder.

4. Denegación de servicio a través del IFD Offset en archivos TIFF

El archivo TIFF consiste en múltiples entradas Image File Directory (IFD), cada una describiendo una imagen específica. Al final de la estructura IFD, existe un valor

DWORD que indica el desplazamiento del siguiente directorio (0 en caso de que sea el último).

Si modificamos el valor del desplazamiento del primer directorio para que apunte a sí mismo, esto hará que el procesador de imágenes de IrfanView entre en un bucle infinito, dando lugar a una denegación de servicio.

5. Estatus y conclusiones

Las vulnerabilidades han sido confirmadas para IrfanView v.4.20 aunque todas las versiones anteriores también podrían verse afectadas.

IrfanView v.4.23 no se ve afectado.

6. En la web

Hispacec Sistemas

<http://hispasec.com>

IrfanView

<http://www.irfanview.com/>

Revelación de información basada en imágenes en múltiples navegadores

http://www.hispasec.com/laboratorio/vulnerabilidad_firefox.pdf