



**HISPASEC SISTEMAS**

SEGURIDAD Y TECNOLOGÍAS  
DE LA INFORMACIÓN

**Documento técnico:  
Desbordamiento de búfer en SDL\_Image 1.2.6**

**Enero 2009**

Matthew "j00ru" Jurczyk  
[matthew@hispasec.com](mailto:matthew@hispasec.com)

## 1. Introducción

SDL\_Image es una librería gratuita y de código abierto que extiende la funcionalidad de SDL, dando soporte a múltiples formatos gráficos, tales como: BMP, GIF, JPEG, LBM, PCX, PNG, PNM, TGA, TIFF, XCF, XPM y XV.

Se ha encontrado una vulnerabilidad de desbordamiento de búfer en el archivo IMG\_bmp.c de SDL\_Image que podría ser aprovechado por un atacante remoto para causar una denegación de servicio y, potencialmente, lograr la ejecución de código arbitrario si un usuario intenta abrir un archivo especialmente manipulado.

El archivo IMG\_bmp.c es el responsable del manejo de los datos de los archivos Bitmap, incluyendo la descompresión de RLE8, en la que estamos especialmente interesados.

## 2. Detalles

Esta sección muestra el análisis detallado de la porción de código vulnerable al desbordamiento de búfer, que tendría lugar en los siguientes bucles al copiar 'ch' número de bytes al búfer de destino:

```
do {  
  
    bits[ofs++] = pixel;  
  
} while (--ch);
```

junto con

```
do {  
  
    if ( !SDL_RWread(src, bits + ofs++, 1, 1) ) return 1;  
  
} while (--ch);
```

El array bits[] es un puntero a surface (búfer de píxeles), creado en:

```
surface = SDL_CreateRGBSurface(SDL_SWSURFACE,  
  
    biWidth, biHeight, biBitCount, Rmask, Gmask, Bmask, Amask);
```

Si el tamaño del búfer es reservado de tal forma que puede almacenar una imagen de un píxel pero allí se copian 255 bytes, entonces tendría lugar un desbordamiento de búfer basado en heap.

Es recomendable añadir algún tipo de código de comprobación si el rango del búfer de la imagen actual no se ha llenado antes de copiar los siguientes bytes en dicho búfer.

La vulnerabilidad podría ser explotada si le damos a la anchura de la imagen un valor menor que 255 y hacemos que los datos de la imagen se parezcan a "\xFF\x00\x00\x01", lo que significaría:

- \* Copiar 255 veces el valor \0.
- \* Final del marcador de bitmap.

Obviamente esto causaría una denegación de servicio, pero sustituyendo los ceros por ciertos datos especialmente manipulados se podría lograr la ejecución de código arbitrario.

### 3. Estatus y conclusiones

La vulnerabilidad ha sido confirmada para SDL\_Image v.1.2.6 aunque todas las versiones anteriores también podrían verse afectadas.

SDL\_Image v.1.2.7 no se ve afectado.

### 4. En la Web

Hispacec Sistemas

<http://hispacec.com>

SDL\_image 1.2

[http://www.libSDL.org/projects/SDL\\_image/](http://www.libSDL.org/projects/SDL_image/)