



HISPASEC SISTEMAS

SEGURIDAD Y TECNOLOGÍAS
DE LA INFORMACIÓN

**White paper:
Buffer overflow in SDL_Image 1.2.6**

January 2009

Matthew "j00ru" Jurczyk
matthew@hispasec.com

1. Introduction

SDL_Image is a freeware, opensource extension library for SDL, supporting a number of various graphic formats, such as: BMP, GIF, JPEG, LBM, PCX, PNG, PNM, TGA, TIFF, XCF, XPM and XV.

A buffer overflow vulnerability has been found in the IMG_bmp.c file which might be exploited by a remote attacker to cause a denial of service, and potentially lead to arbitrary code execution if a user opens a specially crafted file.

The IMG_bmp.c file is responsible for handling the Bitmap files' data, including the RLE8 decompression, which we are interested in.

2. Vulnerability details

This section shows the detailed analysis of the sample code vulnerable to the buffer overflow, that may occur in the following loops while copying 'ch' number of bytes to the destination buffer:

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

and

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

The bits[] array is a pointer to surface (pixels buffer), created at:

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

If the buffer's size is allocated so as to be able to hold data for 1 pixel image, and then 255 bytes are copied there, a heap-based overflow is likely to take place.

It is advised to add some code checking if the current image buffer range has not exceeded before copying the next bytes to it.

The vulnerability can be exploited by setting the image width to less than 255 and making the image data to look like "\xFF\x00\x00\x01", meaning:

* Copy the \0 value 255 times.

* End of bitmap marker

This would obviously lead to a Denial of Service condition, but copying some specially crafted data instead of zeros could lead to potential code execution.

3. Status and conclusions

The vulnerability has been confirmed for SDL_Image v.1.2.6, but older versions could also be affected.

SDL_Image v.1.2.7 is not affected.

4. Websites

Hispacec Sistemas

<http://hispacec.com>

SDL_image 1.2

http://www.libsdl.org/projects/SDL_image/