CVE-2017-7865

描述：FFmpeg before 2017-01-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the ipvideo\_decode\_block\_opcode\_0xA function in libavcodec/interplayvideo.c and the avcodec\_align\_dimensions2 function in libavcodec/utils.c.

软件：FFmpeg before 2017-01-24

源码：libavcodec/utils.c.

出现位置： 376-382行

关键源码：

超出边界写入 找不到具体位置

@@ -376,6 +376,10 @@ void avcodec\_align\_dimensions2(AVCodecContext \*s, int \*width, int \*height,

w\_align = 4;

h\_align = 4;

}

+ if (s->codec\_id == AV\_CODEC\_ID\_INTERPLAY\_VIDEO) {

+ w\_align = 8;

+ h\_align = 8;

+ }

break;

case AV\_PIX\_FMT\_PAL8:

case AV\_PIX\_FMT\_BGR8:

@@ -385,7 +389,8 @@ void avcodec\_align\_dimensions2(AVCodecContext \*s, int \*width, int \*height,

w\_align = 4;

h\_align = 4;

}

- if (s->codec\_id == AV\_CODEC\_ID\_JV) {

+ if (s->codec\_id == AV\_CODEC\_ID\_JV ||

+ s->codec\_id == AV\_CODEC\_ID\_INTERPLAY\_VIDEO) {

w\_align = 8;

h\_align = 8;

}