CVE-2016-10064

描述：Buffer overflow in coders/tiff.c in ImageMagick before 6.9.5-1 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.

软件： ImageMagick before 6.9.5-1

源码：coders/tiff.c

出现位置：1903-1917行、2012-2026行

关键源码：

#include "magick/log.h"

#include "magick/magick.h"

#include "magick/memory\_.h"

+#include "magick/memory-private.h"

#include "magick/module.h"

#include "magick/monitor.h"

#include "magick/monitor-private.h"

@@ -1903,14 +1904,13 @@ RestoreMSCWarning

}

(void) SetImageStorageClass(image,DirectClass);

number\_pixels=(MagickSizeType) columns\*rows;

- if ((number\_pixels\*sizeof(uint32)) != (MagickSizeType) ((size\_t)

- (number\_pixels\*sizeof(uint32))))

+ if (HeapOverflowSanityCheck(rows,sizeof(\*tile\_pixels)) != MagickFalse)

{

TIFFClose(tiff);

ThrowReaderException(ResourceLimitError,"MemoryAllocationFailed");

}

- tile\_pixels=(uint32 \*) AcquireQuantumMemory(number\_pixels,

- sizeof(\*tile\_pixels));

+ tile\_pixels=(uint32 \*) AcquireQuantumMemory(columns,

+ rows\*sizeof(\*tile\_pixels));

if (tile\_pixels == (uint32 \*) NULL)

{

TIFFClose(tiff);

@@ -2012,14 +2012,13 @@ RestoreMSCWarning

Convert TIFF image to DirectClass MIFF image.

\*/

number\_pixels=(MagickSizeType) image->columns\*image->rows;

- if ((number\_pixels\*sizeof(uint32)) != (MagickSizeType) ((size\_t)

- (number\_pixels\*sizeof(uint32))))

+ if (HeapOverflowSanityCheck(image->rows,sizeof(\*pixels)) != MagickFalse)

{

TIFFClose(tiff);

ThrowReaderException(ResourceLimitError,"MemoryAllocationFailed");

}

pixel\_info=AcquireVirtualMemory(image->columns,image->rows\*

- sizeof(uint32));

+ sizeof(\*pixels));

if (pixel\_info == (MemoryInfo \*) NULL)

{

TIFFClose(tiff);