CVE-2017-5974

描述：Heap-based buffer overflow in the \_\_zzip\_get32 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.

软件：zziplib 0.13.62

源码：zzip/fetch.c

出现位置： 32行

关键源码：

\_\_zzip\_get32(unsigned char \*s)

{

#if defined \_\_ZZIP\_GET32

return \_\_ZZIP\_GET32(s);

#else

return ((uint32\_t) s[3] << 24) | ((uint32\_t) s[2] << 16)

| ((uint32\_t) s[1] << 8) | ((uint32\_t) s[0]); // heap-buffer-overflow

#endif

}