CVE-2017-6965

描述：readelf in GNU Binutils 2.28 writes to illegal addresses while processing corrupt input files containing symbol-difference relocations, leading to a heap-based buffer overflow.

软件：GNU Binutils 2.28

源码：binutils/elfcomm.c

出现位置： 75行

关键源码：

byte\_put\_little\_endian (unsigned char \* field, elf\_vma value, int size)

{

switch (size)

{

case 8:

field[7] = (((value >> 24) >> 24) >> 8) & 0xff;

field[6] = ((value >> 24) >> 24) & 0xff;

field[5] = ((value >> 24) >> 16) & 0xff;

field[4] = ((value >> 24) >> 8) & 0xff;

/\* Fall through. \*/

case 4:

field[3] = (value >> 24) & 0xff;

/\* Fall through. \*/

case 3:

field[2] = (value >> 16) & 0xff;

/\* Fall through. \*/

case 2:

field[1] = (value >> 8) & 0xff;

/\* Fall through. \*/

case 1:

field[0] = value & 0xff;

break;

default:

error (\_("Unhandled data length: %d\n"), size);

abort ();

}