CVE-2017-6448

描述：The dalvik\_disassemble function in libr/asm/p/asm\_dalvik.c in radare2 1.2.1 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted DEX file.

软件：radare

源码：libr/asm/p/asm\_dalvik.c

出现位置： 26-410行

关键源码：

stack-based buffer overflow

case 0x01: /\* packed-switch-payload \*/

// ushort size

// int first\_key

// int[size] = relative offsets

{

unsigned short array\_size = buf[2] | (buf[3] << 8);

int first\_key = buf[4] | (buf[5] << 8) | (buf[6] << 16) | (buf[7] << 24);

sprintf (op->buf\_asm, "packed-switch-payload %d, %d", array\_size, first\_key);

size = 8;

payload = 2 \* (array\_size \* 2);

len = 0;

}

break;

case 0x02: /\* sparse-switch-payload \*/

.......