CVE-2017-6194

描述：The relocs function in libr/bin/p/bin\_bflt.c in radare2 1.2.1 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file.

软件：radare2 1.2.1

源码：libr/bin/p/bin\_bflt.c

出现位置： 166-182行

关键源码：

循环复制

struct reloc\_struct\_t \*got\_table = calloc (1, n\_got \* sizeof (ut32));

if (got\_table) {

ut32 offset = 0;

for (i = 0; i < n\_got ; offset += 4, i++) {

ut32 got\_entry;

if (obj->hdr->data\_start + offset + 4 > obj->size ||

obj->hdr->data\_start + offset + 4 < offset) {

break;

}

len = r\_buf\_read\_at (obj->b, obj->hdr->data\_start + offset,

(ut8 \*)&got\_entry, sizeof (ut32));

if (!VALID\_GOT\_ENTRY (got\_entry) || len != sizeof (ut32)) {

break;

}

got\_table[i].addr\_to\_patch = got\_entry;

got\_table[i].data\_offset = got\_entry + BFLT\_HDR\_SIZE;

}