CVE-2017-6319

描述：The dex\_parse\_debug\_item function in libr/bin/p/bin\_dex.c in radare2 1.2.1 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted DEX file.

软件：radare2 1.2.1

源码：libr/bin/p/bin\_dex.c

出现位置： 312-338行

关键源码：

if (argReg >= regsz) {

//return; // this return breaks tests

}

p4 = r\_uleb128 (p4, p4\_end - p4, &line\_start);

p4 = r\_uleb128 (p4, p4\_end - p4, &parameters\_size);

// TODO: check when we should use source\_file

// The state machine consists of five registers

ut32 address = 0;

ut32 line = line\_start;

if (!(debug\_positions = r\_list\_newf ((RListFree)free))) {

return;

}

if (!(emitted\_debug\_locals = r\_list\_newf ((RListFree)free))) {

r\_list\_free (debug\_positions);

return;

}

struct dex\_debug\_local\_t debug\_locals[regsz];

memset (debug\_locals, 0, sizeof (struct dex\_debug\_local\_t) \* regsz);

if (!(MA & 0x0008)) {

debug\_locals[argReg].name = "this"; //overflow here

debug\_locals[argReg].descriptor = r\_str\_newf("%s;", class\_name);

debug\_locals[argReg].startAddress = 0;

debug\_locals[argReg].signature = NULL;

debug\_locals[argReg].live = true;

argReg++;

}