CVE-2017-6439

描述：Heap-based buffer overflow in the parse\_string\_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds write) via a crafted plist file.

软件：libplist 1.12

源码：libplist/src/bplist.c

出现位置：287-303行

关键源码：

static plist\_t parse\_string\_node(const char \*\*bnode, uint64\_t size)

{

plist\_data\_t data = plist\_new\_plist\_data();

data->type = PLIST\_STRING;

data->strval = (char \*) malloc(sizeof(char) \* (size + 1));

if (!data->strval) {

plist\_free\_data(data);

PLIST\_BIN\_ERR("%s: Could not allocate %" PRIu64 " bytes\n", \_\_func\_\_, sizeof(char) \* (size + 1));

return NULL;

}

memcpy(data->strval, \*bnode, size); // buffer overflow

data->strval[size] = '\0';

data->length = strlen(data->strval);

return node\_create(NULL, data);

}