CVE-2017-6438

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

软件：libplist 1.12

源码：libplist/src/bplist.c

出现位置： 383、384行

关键源码：

循环复制

for (i = 0; i < size; i++)

unicodestr[i] = be16toh(((uint16\_t\*)\*bnode)[i]);