New issue

Jump to bottom

Buffer overflow causing RCE in readelf #243

Closed liyansong2018 opened this issue on Jun 10 · 0 comments

liyansong2018 commented on Jun 10

Hi,

readelf in ToaruOS 2.0.1 has a global overflow allowing RCE when parsing a crafted ELF file. Through elaborately constructed elf files, remote code execution can be realized.

PoC

```
./readelf -d poc_elf_overflow

Dynamic section at offset 0x2df8 contains (up to) 30 entries:
  Tag        Type                         Name/Value
zsh: segmentation fault  ./readelf -d poc_elf_overflow
```

poc_elf_overflow.zip

Patch

```
$ git diff
diff --git a/apps/readelf.c b/apps/readelf.c
index ce25d5e1..91f5e722 100644
--- a/apps/readelf.c
+++ b/apps/readelf.c
@@ -168,7 +168,7 @@ static char * dynamicTagToStr(Elf64_Dyn * dynEntry, char * dynstr) {
                        break;
                case DT_NEEDED:
                        name = "(NEEDED)";
-                       sprintf(extra, "[shared lib = %s]", dynstr + dynEntry->d_un.d_val);
+                       snprintf(extra, 500, "[shared lib = %s]", dynstr + dynEntry->d_un.d_val);
                        break;
                case DT_PLTRELSZ:
                        name = "(PLTRELSZ)";
@@ -286,7 +286,7 @@ static char * dynamicTagToStr(Elf64_Dyn * dynEntry, char * dynstr) {
                        break;
        }
```

```
-       sprintf(buf,"%-15s %s", name, extra);
+       snprintf(buf, 1024, "%-15s %s", name, extra);
        return buf;
 }
```

 **klange** closed this as completed in `5d36d27` on Aug 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant