New issue

Jump to bottom

Buffer overrun in format_timespan #23928

Closed **yiyuaner** opened this issue on Jul 7 · 0 comments · Fixed by #23933

Labels bug

yiyuaner commented on Jul 7 • edited

systemd version the issue has been seen with

251

Used distribution

No response

Linux kernel version used

No response

CPU architectures issue was seen on

No response

Component

No response

Expected behaviour you didn't see

No response

Unexpected behaviour you saw

In the file `time-util.c`, the function `format_timespan` has the following code:

```
char *format_timespan(char *buf, size_t l, usec_t t, usec_t accuracy) {
    char *p = buf;
    for (size_t i = 0; i < ELEMENTSOF(table); i++) {
        size_t n;
        ....
        if (!done) {
            k = snprintf(p, l,
                                "%s"USEC_FMT"%s",
                                p > buf ? " " : "",
                                a,
                                table[i].suffix);

            t = b;
        }
        n = MIN((size_t) k, l);
        l -= n;
        p += n;
    }
    *p = 0;
    return buf;
}
```

The problem of the above code is that `n = MIN((size_t) k, l);` can assign the buffer size `l` to `n`. Then `p += n;` will cause `p` to point to one byte after the buffer `buf`, leading to a buffer overwrite in `*p=0` (an off-by-one error).

Steps to reproduce the problem

To reproduce the buffer overrun, just run the following test code

```
int main() {
    char buf[5];
    char *p;
    usec_t t = 100005;
    usec_t accuracy = 1000;
    p = format_timespan(buf, sizeof(buf), t, accuracy);
    printf("%s\n",p);
    return 0;
}
```

`format_timespan` will write to `buf[5]`, which is an error.

Additional program output to the terminal or log subsystem illustrating the issue

No response

yuwata added a commit to yuwata/systemd that referenced this issue on Jul 7

 `time-util: fix buffer-over-run` ··· `35ba044`

 **yuwata** mentioned this issue on Jul 7

time-util: fix buffer-over-run #23933

Merged

yuwata added a commit to yuwata/systemd that referenced this issue on Jul 7

 `time-util: fix buffer-over-run` ··· `8d2d089`

 **poettering** closed this as completed in #23933 on Jul 8

---

poettering pushed a commit that referenced this issue on Jul 8

 `time-util: fix buffer-over-run` ··· ✕ `9102c62`

tewarid pushed a commit to tewarid/systemd that referenced this issue on Aug 23

 `time-util: fix buffer-over-run` ··· `72d4c15`

arnout pushed a commit to buildroot/buildroot that referenced this issue 6 days ago

 `package/systemd: security bump to version v250.8` ··· `e24033f`

arnout pushed a commit to buildroot/buildroot that referenced this issue 3 days ago

 `package/systemd: security bump to version v250.8` ··· `d25bad9`

arnout pushed a commit to buildroot/buildroot that referenced this issue 3 days ago

 `package/systemd: security bump to version v250.8` ··· `5ab86ea`

Assignees

No one assigned

Labels

bug 🐛

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

time-util: fix buffer-over-run
yuwata/systemd

---

1 participant