From: Alexander Larkin <avlarkin82@gmail.com>
To: dmitry.torokhov@gmail.com, dan.carpenter@oracle.com,
linux-input@vger.kernel.org, linux-kernel@vger.kernel.org,
security@kernel.org
Cc: Alexander Larkin <avlarkin82@gmail.com>,
Murray McAllister <murray.mcallister@gmail.com>
Subject: [PATCH] Input: joydev - prevent potential write out of bounds in ioctl
Date: Sun, 20 Jun 2021 15:00:30 +0300 [thread overview]
Message-ID: <20210620120030.1513655-1-avlarkin82@gmail.com> (raw)

The problem is that the check of user input values that is just
before the fixed line of code is for the part of first values
(before len or before len/2), but then the usage of all the values
including i >= len (or i >= len/2) could be.
Since the resulted array of values inited by default with some
good values, the fix is to ignore out of bounds values and
just to use only correct input values by user.
Originally detected by Murray with this simple poc
(If you run the following as an unprivileged user on a default install
it will instantly panic the system:

```
int main(void) {
        int fd, ret;
        unsigned int buffer[10000];

        fd = open("/dev/input/js0", O_RDONLY);
        if (fd == -1)
                printf("Error opening file\n");

        ret = ioctl(fd, JSIOCSBTNMAP & ~IOCSIZE_MASK, &buffer);
        printf("%d\n", ret);
}
```

Fixes: 182d679b2298 ("Input: joydev - prevent potential read overflow in ioctl")
Reported-by: Murray McAllister <murray.mcallister@gmail.com>
Signed-off-by: Alexander Larkin <avlarkin82@gmail.com>
---
drivers/input/joydev.c | 4 ++--
1 file changed, 2 insertions(+), 2 deletions(-)

```
diff --git a/drivers/input/joydev.c b/drivers/input/joydev.c
index da8963a9f044..1aa067d4a3e8 100644
--- a/drivers/input/joydev.c
+++ b/drivers/input/joydev.c
@@ -464,7 +464,7 @@ static int joydev_handle_JSIOCSAXMAP(struct joydev *joydev,

        memcpy(joydev->abspam, abspam, len);

-       for (i = 0; i < joydev->nabs; i++)
+       for (i = 0; i < len && i < joydev->nabs; i++)
                joydev->absmap[joydev->abspam[i]] = i;

  out:
@@ -498,7 +498,7 @@ static int joydev_handle_JSIOCSBTNMAP(struct joydev *joydev,

        memcpy(joydev->keypam, keypam, len);

-       for (i = 0; i < joydev->nkey; i++)
+       for (i = 0; i < (len / 2) && i < joydev->nkey; i++)
                joydev->keymap[keypam[i] - BTN_MISC] = i;

  out:
--
2.27.0
```

---

next reply other threads:[~2021-06-20 12:01 UTC|newest]

Thread overview: 10+ messages / expand[flat|nested] mbox.gz Atom feed top
2021-06-20 12:00 Alexander Larkin [this message]
2021-06-20 16:37 ` [PATCH] Input: joydev - prevent potential write out of bounds in ioctl Linus Torvalds
2021-06-21 5:25 ` Dmitry Torokhov
2021-06-21 15:45 ` Linus Torvalds
2021-06-21 20:06 ` Alexander Larkin
2021-06-21 21:30 ` Alexander Larkin
2021-06-21 21:32 ` Alexander Larkin
2021-06-21 22:38 ` Dmitry Torokhov
2021-07-03 16:21 ` Denis Efremov
2021-07-05 10:54 ` Dan Carpenter

find likely ancestor, descendant, or conflicting patches for this message:
dfblob:da8963a9f04 dfblob:1aa067d4a3e
search (help)

Reply instructions:

You may reply publicly to this message via plain-text email
using any one of the following methods:

* Save the following mbox file, import it into your mail client,
and reply-to-all from there: mbox

Avoid top-posting and favor interleaved quoting:
https://en.wikipedia.org/wiki/Posting_style#Interleaved_style

* Reply using the **--to**, **--cc**, and **--in-reply-to**
switches of git-send-email(1):

```
git send-email \
  --in-reply-to=20210620120030.1513655-1-avlarkin82@gmail.com \
  --to=avlarkin82@gmail.com \
  --cc=dan.carpenter@oracle.com \
  --cc=dmitry.torokhov@gmail.com \
  --cc=linux-input@vger.kernel.org \
  --cc=linux-kernel@vger.kernel.org \
  --cc=murray.mcallister@gmail.com \
  --cc=security@kernel.org \
  /path/to/YOUR_REPLY
```

https://kernel.org/pub/software/scm/git/docs/git-send-email.html

* If your mail client supports setting the **In-Reply-To** header
via mailto: links, try the mailto: link

Be sure your reply has a **Subject:** header at the top and a blank line before the message body.
