**Bug Report**

Reporter: Huang Wenjie

Email: [wenjiezander@gmail.com](mailto:wenjiezander@gmail.com)

Library Name: Recutils

Version: 1.8

Component: csv2rec

Operating System: Ubuntu 20.04.2 LTS

Download link for crash seed: https://drive.google.com/file/d/1zEzaZt-JKqAncYNcnQ6ivJGaNvzmCxEa/view?usp=sharing

Bug found (Fig. 1):

Deference of a high value address.

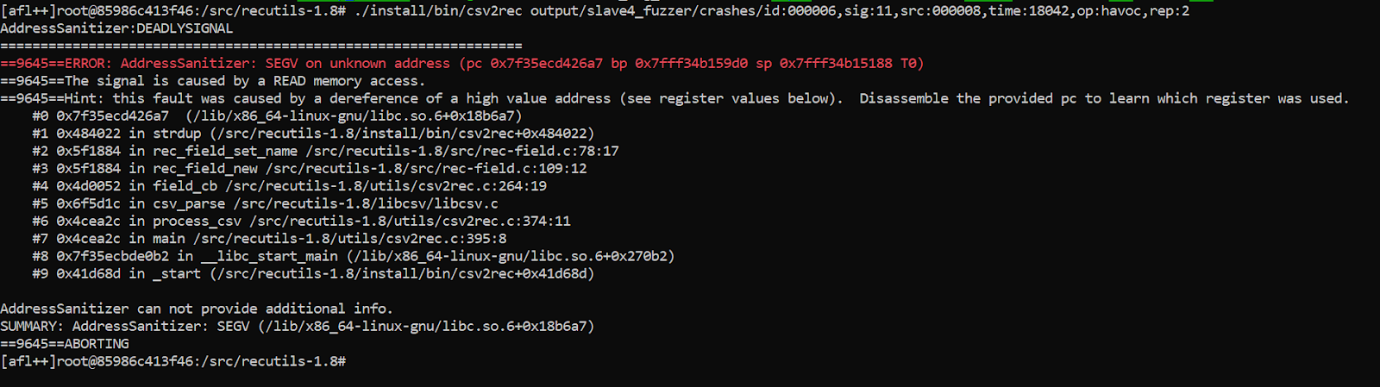


Fig. 1

Steps to reproduce the bug:

1. In recutils-1.8, compile csv2rec into a binary executable
   1. ./configure
   2. make
   3. make install
2. Run the executable with the crash\_seed (A download link for the crash seed is provided above)
   1. ./csv2rec crash\_seed

Observation:

The variable “name” with an invalid address is passed  in to the function “rec\_field\_set\_name” in “recutils-1.8/src/rec-field.c:109” and the function “strdup” in “rec\_field\_set\_name” tries to read from the invalid address which results in a deference of a high value address. A proof of the invalid address is shown in Fig. 2.

Further investigation is required to examine the reason that this invalid address is produced.

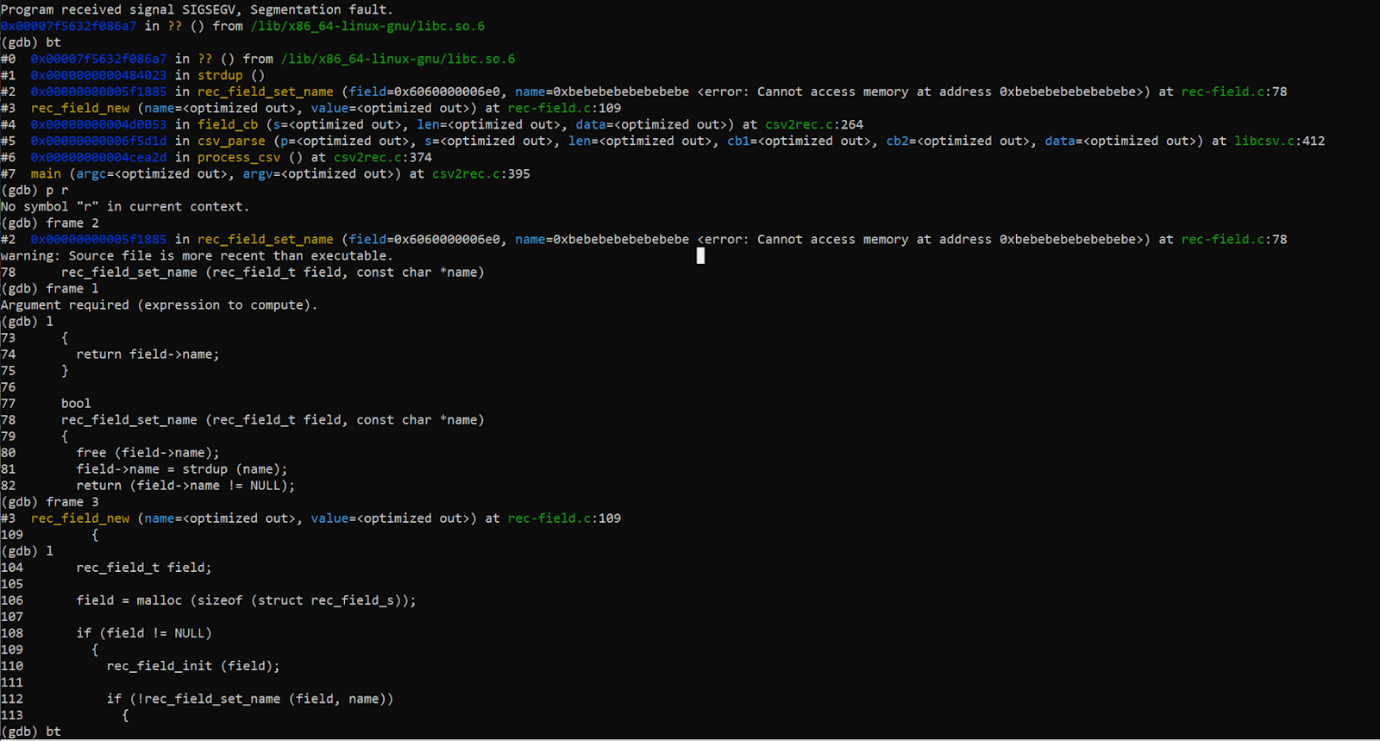


Fig. 2