

MariaDB server crash at my_decimal::operator=

Details

Type: Dug

Status: CLOSED (View Workflow)

Affects Version/s: 10.6.0, 10.6.1, 10.6.2, 10.6.3

Fix Version/s: N/A

Component/s: Optimizer

Labels: (crash)

Environment: Linux 5.4.0-39-generic #43-Ubuntu SMP Fri Jun 19 10:28:31 UTC 2020 x86_64

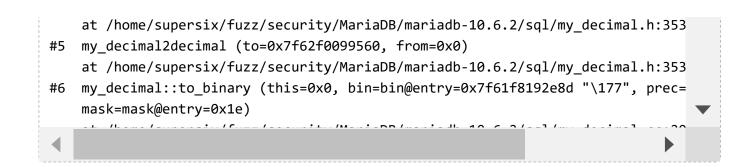
x86_64 x86_64 GNU/Linux

Description

step to reproduce:

```
CREATE TABLE v0 ( v1 INTEGER UNIQUE , v2 INT UNIQUE );
INSERT INTO v0 ( v2 , v1 ) VALUES ( 26 , 8 );
UPDATE v0 SET v1 = CASE 41219694.000000 WHEN 0 THEN 'x' WHEN 'x' THEN 'x' END ORDE
```

Core was generated by `home/supersix/fuzz/security/MariaDB/install/bin/mysqld --defaults-file=/home/s'.Program terminated with signal SIGSEGV, Segmentation fault.



Issue Links

duplicates

MDEV-25994 Crash with union of my_decimal type in ORDER BY clause



CLOSED

links to

CVE-2022-27380

Activity

▼ ○ Alice Sherepa added a comment - 2021-07-30 13:50

Thanks for the report!

This is the same issue as MDEV-25994

People

Assignee:

Unassigned

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2021-07-30 10:08

Updated:

2022-04-13 13:00

Resolved:

∨ Git Integration

• Error rendering 'com.xiplink.jira.git.jira_git_plugin:git-issue-webpanel'. Please contact your Jira administrators.