MariaDB Server MDEV-26280

MariaDB server crash at my_decimal::operator=

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Major
Resolution:	Duplicate
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.

```
#0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0xb)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
56      ../sysdeps/unix/sysv/linux/pthread_kill.c: No such file or directory.

[Current thread is 1 (Thread 0x7f62f009b700 (LWP 166191))]
gdb-peda$ bt
#0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0xb)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
#1  0x000055fcfb78307f in my_write_core (sig=sig@entry=0xb)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/mysys/stacktrace.c:4
#2  0x000055fcfb107f80 in handle_fatal_signal (sig=0xb)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/signal_handler.c
#3  <signal handler called>
#4  0x000055fcfb26d753 in my_decimal::operator= (rhs=..., this=0x7f62f0099560)
```

```
     at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/my_decimal.h:353
 #5  my_decimal2decimal (to=0x7f62f0099560, from=0x0)
     at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/my_decimal.h:353
 #6  my_decimal::to_binary (this=0x0, bin=bin@entry=0x7f61f8192e8d "\177", prec=
     mask=mask@entry=0x1e)
```

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:

2021-07-30 13:51

Git Integration

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