MariaDB Server MDEV-26427

# MariaDB Server SEGV on INSERT .. SELECT

## Details

| | |
|---|---|
| Type: | Bug |
| Status: | CLOSED (View Workflow) |
| Priority: | Blocker |
| Resolution: | Fixed |
| Affects Version/s: | 10.7.0, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8 |
| Fix Version/s: | 10.3.36, 10.4.26, 10.5.17, (4) |
| Component/s: | Optimizer - Window functions |
| Labels: | None |
| Environment: | Linux version 5.13.0-1-MANJARO (builduser@LEGION) (gcc (GCC) 11.1.0, GNU ld (GNU Binutils) 2.36.1) #1 SMP PREEMPT Mon Jun 7 06:16:10 UTC 2021 x86_64 |

## Description

step to reproduce:

```
CREATE TABLE v0 ( v1 DECIMAL UNIQUE CHECK ( CASE 0 * 27302337.000000 WHEN 34 THEN +
 INSERT INTO v0 VALUES ( 90 ) , ( -1 ) , ( 31152443.000000 ) , ( -32768 ) , ( NULL
 INSERT INTO v0 SELECT AVG ( 'x' ) OVER ( PARTITION BY ( ( NOT AVG ( 76698761.00000
 INSERT IGNORE INTO v0 ( ) VALUES ( 0 ) , ( 'x' ) , ( 3751286.000000 ) , ( 'x' ) ,
 INSERT INTO v0 VALUES ( 127 ) ;
 INSERT INTO v0 SELECT -2147483648 END FROM v0 AS TEXT JOIN v0 JOIN v0 TABLES ;
 ALTER TABLE v0 ADD ( v2 INT UNIQUE CHECK ( ( v1 = 'x' AND ( ( - ( + ( BINARY 49730
 UPDATE v0 SET v1 = -128 WHERE v1 IS NULL ORDER BY 78 IN ( 'x' , 'x' ) , v1 ;
```

report (compiled with ASAN):

```
This could be because you hit a bug. It is also possible that this binary
or one of the libraries it was linked against is corrupt, improperly built,
or misconfigured. This error can also be caused by malfunctioning hardware.

To report this bug, see https://mariadb.com/kb/en/reporting-bugs

We will try our best to scrape up some info that will hopefully help
diagnose the problem, but since we have already crashed,
something is definitely wrong and this may fail.
```

```
Server version: 10.7.0-MariaDB
key_buffer_size=134217728
read_buffer_size=131072
max_used_connections=1
max_threads=153
thread_count=1
It is possible that mysqld could use up to
key_buffer_size + (read_buffer_size + sort_buffer_size)*max_threads = 467956 K
Hope that's ok; if not, decrease some variables in the equation.
```

gdb bt:

```
#0  0x00007f4afe4ef808 in pthread_kill () from /usr/lib/libpthread.so.0
#1  0x000055a35682706b in handle_fatal_signal (sig=<optimized out>) at /experiment/
#2  <signal handler called>
#3  0x0000000000000000 in ?? ()
#4  0x000055a3561b9ee7 in sub_select (join=0x629000089208, join_tab=0x629000089c88,
#5  0x000055a35625eb8d in do_select (procedure=0x0, join=0x629000089208) at /experi
#6  JOIN::exec_inner (this=0x629000089208) at /experiment/mariadb-server/sql/sql_se
#7  0x000055a356260593 in JOIN::exec (this=this@entry=0x629000089208) at /experimen
#8  0x000055a356258b5b in mysql_select (thd=0x62b0000bd218, tables=<optimized out>,
    at /experiment/mariadb-server/sql/sql_select.cc:4991
#9  0x000055a35625a655 in handle_select (thd=thd@entry=0x62b0000bd218, lex=lex@entr
#10 0x000055a3560c99c1 in mysql_execute_command (thd=0x62b0000bd218, is_called_from
#11 0x000055a3560cc5a1 in mysql_parse (thd=0x62b0000bd218, rawbuf=<optimized out>,
#12 0x000055a3560d260c in dispatch_command (command=<optimized out>, thd=0x62b0000b
#13 0x000055a3560d773d in do_command (thd=0x62b0000bd218, blocking=blocking@entry=t
#14 0x000055a356492e57 in do_handle_one_connection (connect=<optimized out>, put_in
#15 0x000055a35649333d in handle_one_connection (arg=arg@entry=0x6080000023b8) at /
#16 0x000055a356f23c2c in pfs_spawn_thread (arg=0x617000005f18) at /experiment/mari
#17 0x00007f4afe4e8259 in start_thread () from /usr/lib/libpthread.so.0
```

## Issue Links

**links to**

CVE-2022-32084

## Activity

Oleg Smirnov added a comment - 2022-06-14 13:38

Another observation of incorrect behavior - aggregate function returns non-NULL value but NULL is inserted instead.

```
MariaDB [test]> CREATE TABLE t1 (a int);

MariaDB [test]> select avg(9);
+--------+
| avg(9) |
+--------+
| 9.0000 |
+--------+
1 row in set (4.615 sec)

MariaDB [test]> insert into t1 select avg(9);
Query OK, 1 row affected (0.002 sec)
Records: 1  Duplicates: 0  Warnings: 0

MariaDB [test]> select * from t1;
+------+
| a    |
+------+
| NULL |
+------+
1 row in set (5.886 sec)
```

Same with other aggregate functions, for example:

```
select sum(9);
```

---

Oleg Smirnov added a comment - 2022-07-12 12:18 - edited

Pushed into bb-10.3-~~MDEV-26427~~

---

Oleksandr Byelkin added a comment - 2022-07-12 19:16

OK to push

---

Oleg Smirnov added a comment - 2022-07-14 06:24

Pushed to 10.3

## People

Assignee:

Oleg Smirnov

Reporter:

Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

## Dates

Created:

2021-08-19 04:06

Updated:

2022-07-14 06:25

Resolved:

2022-07-14 06:24

## Git Integration

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