





MariaDB Server

MDEV-28081

MariaDB SEGV issue

Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Major
Resolution:	Duplicate
Affects Version/s:	10.9.0
Fix Version/s:	N/A
Component/s:	Optimizer - Window functions
Labels:	None
Environment:	Linux jie-2 5.4.143-1-pve #1 SMP PVE 5.4.143-1 (Tue, 28 Sep 2021 09:10:37 +0200) x86_64 x86_64 x86_64 GNU/Linux

Description

PoC:

```
SELECT AVG ( - NULL ) OVER ( PARTITION BY 'x' / 17709244.000000 ) / + AVG ( FALSE )
```

report:



```
Thread pointer: 0x7fa80400c58
Attempting backtrace. You can use the following information to find out
where mysqld died. If you see no messages after this, something went
terribly wrong...
stack_bottom = 0x7fa8640ebe30 thread_stack 0x49000
mysys/stacktrace.c:212(my_print_stacktrace)[0xe12bae]
sql/signal_handler.cc:226(handle_fatal_signal)[0x973f04]
sigaction.c:0(__restore_rt)[0x7fa8676a23c0]
sql/sql_window.cc:435(compare_order_elements(st_order*, st_order*)) [0x8e4131]
sql/sql_window.cc:588(compare_window_funcs_by_window_specs(Item_window_func*, I

??:(JOIN::make_aggr_tables_info())[0x799500]
??:(JOIN::optimize_stage2())[0x78afdb]
sql/sql_select.cc:2492(JOIN::optimize_inner())[0x7922a2]
??:(JOIN::optimize())[0x78af00]
sql/sql_select.cc:4993(mysql_select(THD*, TABLE_LIST*, List<Item>&, Item*, unsi
select_lex*)) [0x785468]
sql/sql_select.cc:543(handle_select(THD*, LEX*, select_result*, unsigned long))
```

```
sql/sql_parse.cc:6252(execute_sqlcom_select(THD*, TABLE_LIST*)) [0x754fea]
```

▼ Issue Links


duplicates

 [MDEV-19398](#) Assertion `item1->type() == Item::FIELD_ITEM && item2->...  **CLOSED**

links to

 [CVE-2022-27445](#)


▼ Activity

▼  [Alice Sherepa](#) added a comment - 2022-03-18 13:51


Thank you! This is the same as [MDEV-19398](#). I added a test there.

▼ People

Assignee:

 Unassigned

Reporter:

 [Jingzhou Fu](#)

Votes:

0 [Vote for this issue](#)

Watchers:

3 [Start watching this issue](#)

▼ Dates

Created:

2022-03-16 09:17

Updated:

2022-04-27 16:06

Resolved:

2022-03-18 13:50

▼ Git Integration

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