





MariaDB Server

MDEV-28094

Window function in expression in ORDER BY

▼ Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Blocker
Resolution:	Fixed
Affects Version/s:	10.9.0, 10.4, 10.5, 10.6, 10.7, 10.8
Fix Version/s:	10.4.25 , 10.5.16 , 10.6.8 , 10.7.4
Component/s:	Optimizer
Labels:	regression
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 EXISTS ( ( SELECT -1 ORDER BY AVG ( 2147483647 ) OVER ( ROWS BETWEEN UNBOUND
```

report (compiled with ASAN):



```
Thread pointer: 0x62b00015e218
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 = 0x7fd219e69880 thread_stack 0x5fc00
??:0(__interceptor_backtrace)[0x7cbadb]
mysys/stacktrace.c:212(my_print_stacktrace)[0x2a86d37]
sql/signal_handler.cc:0(handle_fatal_signal)[0x15af5d9]
sigaction.c:0(__restore_rt)[0x7fd2406673c0]

sql/field_conv.cc:205(set_field_to_null_with_conversions(Field*, bool))[0x158a6
sql/item.cc:6796(Item::save_decimal_in_field(Field*, bool))[0x164caae]
sql/item.cc:6812(Item::save_in_field(Field*, bool))[0x164ce5a]
sql/sql_list.h:441(base_list_iterator::next_fast())[0x137f492]
??:0(Window_func_runner::exec(THD*, TABLE*, SORT_INFO*))[0x1380b36]
sql/sql_window.cc:3013(Window_funcs_sort::exec(JOIN*, bool))[0x138110a]
??:0(Window_funcs_computation::exec(JOIN*, bool))[0x1383947]
```

```
sql/sql_select.cc:29515(AGGR_OP::end_send())[0xe2fe7f]
sql/sql_select.cc:20806(sub_select_postjoin_aggr(JOIN*, st_join_table*, bool))[0xe2fe7f]
```

▼ Issue Links



relates to

 [MDEV-25630](#) Crash with window function in left expr of IN subquery  **CLOSED**

links to

 [CVE-2022-27451](#)

▼ Activity

▼  [Alice Sherepa](#) added a comment - 2022-03-22 10:10 

Thank you!

the bug is reproducible on 10.4-10.8, while not on 10.2,10.3

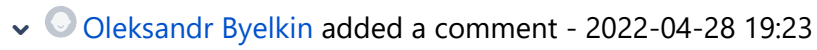
```
#SELECT EXISTS ( ( SELECT -1 ORDER BY AVG ( 2147483647 ) OVER ( ROWS BETWEEN UNBOUNDED PRECEDING AND CURRENT ROW ) ) )
SELECT EXISTS (SELECT 1 ORDER BY 1+sum(2) OVER ());
```

Version: '10.4.25-MariaDB-debug-log'

220322 11:06:10 [ERROR] mysqld got signal 11 ;

Server version: 10.4.25-MariaDB-debug-log

```
sigaction.c:0(__restore_rt)[0x7f70cf4bc3c0]
sql/field.h:1199(Field::set_notnull(long long))[0x56182d234633]
sql/item.cc:6686(Item::save_decimal_in_field(Field*, bool))[0x56182dcf519b]
sql/sql_type.cc:3832(Type_handler_decimal_result::Item_save_in_field(Item*
sql/item.cc:6702(Item::save_in_field(Field*, bool))[0x56182dcf552d]
sql/sql_window.cc:2725(save_window_function_values(List<Item_window_func>&
sql/sql_window.cc:2879(compute_window_func(THD*, List<Item_window_func>&,
sql/sql_window.cc:2980(Window_func_runner::exec(THD*, TABLE*, SORT_INFO*))
sql/sql_window.cc:3008(Window_funcs_sort::exec(JOIN*, bool))[0x56182da7784]
sql/sql_window.cc:3135(Window_funcs_computation::exec(JOIN*, bool))[0x56182da7784]
sql/sql_select.cc:28988(AGGR_OP::end_send())[0x56182d656018]
sql/sql_select.cc:20342(sub_select_postjoin_aggr(JOIN*, st_join_table*, bo
sql/sql_select.cc:20166(do_select(JOIN*, Procedure*)))[0x56182d613c06]
```



▼ People

4 Start watching this issue

2022-04-29 15:08

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