





MariaDB Server

MDEV-26437

Server crashes in Item_args::walk_args

▼ Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Major
Resolution:	Duplicate
Affects Version/s:	10.7.0, 10.2, 10.3, 10.4, 10.5, 10.6
Fix Version/s:	10.3.35 , 10.4.25 , 10.5.16 , (2)
Component/s:	Virtual Columns
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 ( v2 INT NOT NULL , v1 BIGINT AS ( CASE 'x' WHEN CURRENT_USER ( ) THEN  
SELECT v2 AS v3 FROM v0 WHERE v1 LIKE 'x' ESCAPE 'x' ;  
INSERT INTO v0 VALUES ( -128 , NULL , NULL , NULL , NULL , TO_DATE ( 'x' , 'x' ) ) )
```

report (compiled with ASAN):

```
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
 $\text{key_buffer_size} + (\text{read_buffer_size} + \text{sort_buffer_size}) * \text{max_threads} = 467956 \text{ K}$
Hope that's ok; if not, decrease some variables in the equation.

```
Thread pointer: 0x62b0000bd218  
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 = 0x7f9fca453850 thread_stack 0x5fc00
```

```
sanitizer_common/sanitizer_common_interceptors.inc:4203(__interceptor_backtrace
mysys/stacktrace.c:213(my_print_stacktrace)[0x556139072747]
sql/signal_handler.cc:222(handle_fatal_signal)[0x55613803a120]
```



gdb bt:

```
Using host libthread_db library "/usr/lib/libthread_db.so.1".
Core was generated by `/usr/local/mysql/bin//mysqld --port 10005 --datadir=/hom
Program terminated with signal SIGABRT, Aborted.
#0  0x00007f9fe96e6808 in pthread_kill () from /usr/lib/libpthread.so.0
#1  0x000055613803a06b in handle_fatal_signal (sig=<optimized out>) at /experim
#2  <signal handler called>
#3  0x00007f9fe91c8d22 in raise () from /usr/lib/libc.so.6

#4  0x00007f9fe91b2862 in abort () from /usr/lib/libc.so.6
#5  0x00007f9fe9552802 in __gnu_cxx::__verbose_terminate_handler () at /build/g
#6  0x00007f9fe955ec8a in __cxxabiv1::__terminate (handler=<optimized out>) at
#7  0x00007f9fe955ecf7 in std::terminate () at /build/gcc/src/gcc/libstdc++-v3/
#8  0x00007f9fe955fa75 in __cxxabiv1::__cxa_pure_virtual () at /build/gcc/src/g
#9  0x00005561380a4308 in Item::check_type_scalar (this=this@entry=0x6290000894
#10 0x00005561381e2a5b in Item_func::check_argument_types_scalar (this=0x619000
#11 0x00005561381ce34e in Item_func::fix_fields (this=this@entry=0x6190000a3ed8
#12 0x0000556138100700 in Item_func_case::fix_fields (this=0x6190000a3ed8, thd=
#13 0x0000556137be6ee2 in fix_vcol_expr (thd=<optimized out>, vcol=0x61d0000532
#14 0x000055613775e1ca in TABLE::fix_vcol_exprs (this=0x6190000a3298, thd=0x62b
```

▼ Issue Links

duplicates

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

is duplicated by

 [MDEV-26353](#) MariaDB server crash in Arg_comparator::compare_real_fixed  **CLOSED**

 [MDEV-26354](#) MariaDB server crash in Field::set_default - ASAN use after ...  **CLOSED**

 [MDEV-26407](#) Server crashes in Item_func_in::cleanup/Item::cleanup_proc...  **CLOSED**

 [MDEV-26426](#) MariaDB server use-after-poison issue  **CLOSED**

[Show 3 more links](#) (1 is duplicated by, 1 relates to, 1 links to)

▼ Activity

✓  Daniel Black added a comment - 2021-08-20 08:40 - [edited](#)




Thanks for the nice stack traces.

Additional gdb option that expands the arguments some more rather than . . . (for next time. We can work it out for the current ones). Thanks for the bu reports.

additional gdb option

```
set print frame-arguments all
```

✓  Alice Sherepa added a comment - 2021-08-24 16:12 - [edited](#)

Thank you! I repeated as described on current 10.2-10.6.

1)

10.2 1f1d5606e08c928e3da98b

```
#3 <signal handler called>
#4 0x000055a739768e91 in Item_args::walk_args (this=0x7f1ae4035b28, proce
#5 0x000055a7397692db in Item_func_or_sum::walk (this=0x7f1ae4035aa0, pro
#6 0x000055a7398d8a90 in fix_session_vcol_expr (thd=0x7f1ae4000d90, vcol=
#7 0x000055a73975def5 in TABLE::fix_vcol_exprs (this=0x7f1ae4176640, thd=
#8 0x000055a73975e128 in fix_all_session_vcol_exprs (thd=0x7f1ae4000d90,
#9 0x000055a73975e76e in lock_tables (thd=0x7f1ae4000d90, tables=0x7f1ae4
#10 0x000055a73975db4d in open_and_lock_tables (thd=0x7f1ae4000d90, option
#11 0x000055a7397235b9 in open_and_lock_tables (thd=0x7f1ae4000d90, tables
#12 0x000055a7397a6272 in mysql_insert (thd=0x7f1ae4000d90, table_list=0x7
#13 0x000055a7397ce638 in mysql_execute_command (thd=0x7f1ae4000d90) at /1
#14 0x000055a7397d9b42 in mysql_parse (thd=0x7f1ae4000d90, rawbuf=0x7f1ae4
#15 0x000055a7397c7d9d in dispatch_command (command=COM_QUERY, thd=0x7f1ae
#16 0x000055a7397c6898 in do_command (thd=0x7f1ae4000d90) at /10.2/src/sql
#17 0x000055a739922661 in do_handle_one_connection (connect=0x55a73d6fad10
#18 0x000055a7399223c6 in handle_one_connection (arg=0x55a73d6fad10) at /1
#19 0x000055a73a14bec4 in pfs_spawn_thread (arg=0x55a73d6ddfd0) at /10.2/s
#20 0x00007f1b3eec8609 in start_thread (arg=<optimized out>) at nthread cr
```

this is probably the same issue as [MDEV-24176](#).

2) another case, that is derived from the test in description:

```
create table t1 (vi int as ( case 'x' when current_user() then 1 end ) ) ;
select 1 from t1 where vi=1;
show create table t1;
```

10.2 1f1d5606e08c928e3da98b

```
#3 <signal handler called>
```

10.2 1f1d5606e08c928e3da98b

```
#4 0x000055d764778405 in Item::print_parenthesised (this=0x7fec30013898,
#5 0x000055d7647ab009 in Item_func_case::print (this=0x7fec30035178, str=
#6 0x000055d764778459 in Item::print_parenthesised (this=0x7fec30035178,
#7 0x000055d764590630 in Item::print_for_table_def (this=0x7fec30035178,
#8 0x000055d764590991 in Virtual_column_info::print (this=0x7fec300352f8,
#9 0x000055d764574186 in show_create_table (thd=0x7fec30000d90, table_li
#10 0x000055d764571a27 in mysql_d_show_create_get_fields (thd=0x7fec30000d9
#11 0x000055d764571f3e in mysql_d_show_create (thd=0x7fec30000d90, table_li
#12 0x000055d7644ddc0a in mysql_execute_command (thd=0x7fec30000d90) at /1
#13 0x000055d7644e9b42 in mysql_parse (thd=0x7fec30000d90, rawbuf=0x7fec30
#14 0x000055d7644d7d9d in dispatch_command (command=COM_QUERY, thd=0x7fec3
#15 0x000055d7644d6898 in do_command (thd=0x7fec30000d90) at /10.2/src/sql
#16 0x000055d764632661 in do_handle_one_connection (connect=0x55d7679cfd10
#17 0x000055d7646323c6 in handle_one_connection (arg=0x55d7679cfd10) at /1
#18 0x000055d76465bec4 in nfs_spawn_thread (arg=0x55d7679b2fd0) at /10.2/s
```

3)


```
create table t1 (vi int as ( case 'x' when current_user() then 1 end ) ) ;
select 1 from t1 where vi=1;
select 1 from t1 where vi=1;
```

10.2 1f1d5606e08c928e3da98b

210824 18:22:51 [ERROR] mysqld got signal 11 ;
Server version: 10.2.41-MariaDB-debug-log

```
sigaction.c:0(__restore_rt)[0x7f62d0eb73c0]
sql/item.h:4134(Item_args::walk_args(bool (Item::*)(void*), bool, void*))[
sql/item.h:4420(Item_func_or_sum::walk(bool (Item::*)(void*), bool, void*)
sql/table.cc:6809(TABLE::mark_virtual_col(Field*)) [0x564f6a11d2e3]

sql/sql_base.cc:5314(update_field_dependencies(THD*, Field*, TABLE*)) [0x56
sql/sql_base.cc:5651(find_field_in_table(THD*, TABLE*, char const*, unsign
sql/sql_base.cc:5764(find_field_in_table_ref(THD*, TABLE_LIST*, char const
sql/sql_base.cc:6056(find_field_in_tables(THD*, Item_ident*, TABLE_LIST*,
sql/item.cc:5463(Item_field::fix_fields(THD*, Item**)) [0x564f6a2b0090]
sql/item_func.cc:201(Item_func::fix_fields(THD*, Item**)) [0x564f6a306295]
sql/sql_base.cc:8004(setup_conds(THD*, TABLE_LIST*, List<TABLE_LIST>&, Ite
sql/sql_select.cc:649(setup_without_group(THD*, Bounds_checked_array<Item*
sql/sql_select.cc:812(JOIN::prepare(TABLE_LIST*, unsigned int, Item*, unsi
```

✓  Alice Sherepa added a comment - 2021-08-25 09:32 - edited

from [MDEV-26432](#), with LIKE function

```
CREATE TABLE t1 ( v2 INT , v1 INT AS (( USER () LIKE 'x' ) ) ) ;
SELECT 1 FROM t1 WHERE v1=1 ;
SELECT * FROM t1;
```

10.2 1f1d5606e08c928e3da98b

```
#3 <signal handler called>
#4 0x000055993dc9de91 in Item_args::walk_args (this=0x7f9c20035278, proce
#5 0x000055993e0f80b7 in Item_func_like::walk (this=0x7f9c200351f0, proce
#6 0x000055993de182e3 in TABLE::mark_virtual_col (this=0x7f9c20175dc0, fi
#7 0x000055993dc99ed2 in insert_fields (thd=0x7f9c20000d90, context=0x7f9
#8 0x000055993dc981dd in setup_wild (thd=0x7f9c20000d90, tables=0x7f9c200
#9 0x000055993dd41931 in JOIN::prepare (this=0x7f9c20013000, tables_init=
#10 0x000055993dd4c51a in mysql_select (thd=0x7f9c20000d90, tables=0x7f9c2
#11 0x000055993dd40720 in handle_select (thd=0x7f9c20000d90, lex=0x7f9c200
#12 0x000055993dd0ad86 in execute_sqlcom_select (thd=0x7f9c20000d90, all_t
#13 0x000055993dd018fa in mysql_execute_command (thd=0x7f9c20000d90) at /1
#14 0x000055993dd0eb42 in mysql_parse (thd=0x7f9c20000d90, rawbuf=0x7f9c20
#15 0x000055993dcfcd9d in dispatch_command (command=COM_QUERY, thd=0x7f9c2
#16 0x000055993dcfb898 in do_command (thd=0x7f9c20000d90) at /10.2/src/sql
#17 0x000055993de57661 in do_handle_one_connection (connect=0x559940c2fac0
#18 0x000055993de573c6 in handle_one_connection (arg=0x559940c2fac0) at /1
#19 0x000055993e680ec4 in pfs_spawn_thread (arg=0x559940c12d80) at /10.2/s
#20 0x00007f9c80f5b609 in start_thread (arg=<optimized out>) at pthread cr
```

```
CREATE TABLE t1 (v2 INT AS ( USER () LIKE 'x')) ;
SELECT 1 FROM t1 ORDER BY v2 ;
ALTER TABLE t1 ADD i int;
```

10.2 1f1d5606e08c928e3da98b

```
#3 <signal handler called>
#4 0x000055cf0812ce91 in Item_args::walk_args (this=0x7f59e8035960, proce
#5 0x000055cf085870b7 in Item_func_like::walk (this=0x7f59e80358d8, proce
#6 0x000055cf0825e0d1 in mysql_prepare_create_table (thd=0x7f59e8000d90,
#7 0x000055cf0825fac6 in mysql_create_frm_image (thd=0x7f59e8000d90, db=0
#8 0x000055cf0826057a in create_table_impl (thd=0x7f59e8000d90, orig_db=0
#9 0x000055cf0826c8d1 in mysql_alter_table (thd=0x7f59e8000d90, new_db=0x
#10 0x000055cf082ebc6c in Sql_cmd_alter_table::execute (this=0x7f59e8012ef
#11 0x000055cf08198cdc in mysql_execute_command (thd=0x7f59e8000d90) at /1
#12 0x000055cf0819db42 in mysql_parse (thd=0x7f59e8000d90, rawbuf=0x7f59e8
```

```
#13 0x000055cf0818bd9d in dispatch_command (command=COM_QUERY, thd=0x7f59e1f1d5606e08c928e3da98b)
#14 0x000055cf0818a898 in do_command (thd=0x7f59e8000d90) at /10.2/src/sql
#15 0x000055cf082e6661 in do_handle_one_connection (connect=0x55cf0b5ead10)
#16 0x000055cf082e63c6 in handle_one_connection (arg=0x55cf0b5ead10) at /1
#17 0x000055cf08b0fec4 in pfs_spawn_thread (arg=0x55cf0b5cdfd0) at /10.2/s
#18 0x00007f5a3c9cd609 in start_thread (arg=<optimized out>) at pthread_cr
#19 0x00007f5a3c5a8293 in clone () at ../sysdeps/unix/sysv/linux/x86_64/cl
```

▼ People

Assignee:



Nikita Malyavin

Reporter:



Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

4 Start watching this issue

▼ Dates

Created:

2021-08-19 04:46

Updated:

2022-07-02 07:38

Resolved:

2021-10-01 19:17

▼ Git Integration



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