MariaDB Server MDEV-26423

MariaDB server crash in Create_tmp_table::finalize

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Fixed
Affects Version/s:	10.2, 10.3, 10.4, 10.5, 10.6, 10.7
Fix Version/s:	10.2.44, 10.3.35, 10.4.25, (5)
Component/s:	OTHER
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 ( v2 DATE DEFAULT ( v1 MOD 68321183.000000 ) , v1 DATETIME NULL ) ;
 SHOW DATABASES LIKE 'x' ;
 SELECT DISTINCT v2 , v1 , DEFAULT ( v2 ) FROM v0 ;
```

Crash Log:

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
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 = 0x7fbccf9b6850 thread_stack 0x5fc00
sanitizer_common/sanitizer_common_interceptors.inc:4203(__interceptor_backtrace
mysys/stacktrace.c:213(my_print_stacktrace)[0x55da8b1e8747]
sql/signal_handler.cc:222(handle_fatal_signal)[0x55da8a1b0120]
sigaction.c:0(__restore_rt)[0x7fbcf4dd3870]
```

Issue Links

relates to

MDEV-11590 Server crashes in create_tmp_table / JOIN::create_postjoin_... CLOSED

links to

CVE-2022-27378

Activity

Alice Sherepa added a comment - 2021-08-25 13:52

Thanks!
Repeatable on 10.2-10.6

```
CREATE TABLE t1 (v1 DATE, v2 DATE DEFAULT(v1)) engine=innodb;
SELECT DISTINCT DEFAULT(v2) FROM t1 ;
```

10.2 1f1d5606e08c928e3da98b

```
#3  <signal handler called>
#4  0x000055b9f38681c4 in create_tmp_table (thd=0x7f540c000d90, param=0x7f
#5  0x000055b9f3842ab9 in JOIN::create_postjoin_aggr_table (this=0x7f540c0
#6  0x000055b9f384130e in JOIN::make_aggr_tables_info (this=0x7f540c013158
#7  0x000055b9f383fec8 in JOIN::optimize_inner (this=0x7f540c013158) at /1
#8  0x000055b9f383bfe6 in JOIN::optimize (this=0x7f540c013158) at /10.2/sr
#9  0x000055b9f384553c in mysql_select (thd=0x7f540c000d90, tables=0x7f540
#10 0x000055b9f3839720 in handle_select (thd=0x7f540c000d90, lex=0x7f540c0


#11 0x000055b9f3803d86 in execute_sqlcom_select (thd=0x7f540c000d90, all_t
#12 0x000055b9f37fa8fa in mysql_execute_command (thd=0x7f540c000d90) at /1
#13 0x000055b9f3807b42 in mysql_parse (thd=0x7f540c000d90, rawbuf=0x7f540c
#14 0x000055b9f37f5d9d in dispatch_command (command=COM_QUERY, thd=0x7f540
#15 0x000055b9f37f4898 in do_command (thd=0x7f540c000d90) at /10.2/src/sql
```

```
10.2 1f1d5066e08c938c3da98b
#16 0x000055b9f3950661 in do_handle_one_connection (connect=0x55b9f70feac0
#17 0x000055b9f39503c6 in handle_one_connection (arg=0x55b9f70feac0) at /1
#18 0x000055b9f4179ec4 in pfs_spawn_thread (arg=0x55b9f70e1d80) at /10.2/s
```

Alice Sherepa added a comment - 2021-10-28 13:16

```
CREATE TABLE t1 (pk varchar(36) DEFAULT uuid());
INSERT INTO t1 VALUES (),();

SELECT 1 FROM t1 GROUP BY DEFAULT(pk);
```

10.6 1193a793c40b806c6f1f00

```
211028 15:14:26 [ERROR] mysqld got signal 11 ;

Server version: 10.6.5-MariaDB-debug-log

sql/signal_handler.cc:226(handle_fatal_signal)[0x55cb38ca7a5b]
sigaction.c:0(__restore_rt)[0x7f6fb1a653c0]
sql/sql_select.cc:19315(Create_tmp_table::finalize(THD*, TABLE*, TMP_TABLE
sql/sql_select.cc:19618(create_tmp_table(THD*, TMP_TABLE_PARAM*, List<Item
sql/sql_select.cc:4012(JOIN::create_postjoin_aggr_table(st_join_table*, Li
sql/sql_select.cc:3591(JOIN::make_aggr_tables_info())[0x55cb38519882]
sql/sql_select.cc:3227(JOIN::optimize_stage2())[0x55cb38515304]
sql/sql_select.cc:2479(JOIN::optimize_inner())[0x55cb3850d944]
sql/sql_select.cc:1809(JOIN::optimize())[0x55cb38506700]
sql/sql_select.cc:4980(mysql_select(THD*, TABLE_LIST*, List<Item>&, Item*,
sql/sql_select.cc:545(handle_select(THD*, LEX*, select_result*, unsigned l
sql/sql_parse.cc:6256(execute_sqlcom_select(THD*, TABLE_LIST*))[0x55cb3845
sql/sql_parse.cc:3946(mysql_execute_command(THD*, bool))[0x55cb3844beb5]
sql/sql_parse.cc:8030(mysql_parse(THD*, char*, unsigned int, Parser_state*
```

Oleksandr Byelkin added a comment - 2022-04-14 11:04 - edited

Using innodb is really needed:

- with innodb we endup trying to get temporary table field from "default" (Item_default_value) item.
- with aria it is normal "result filed" and return temporary table field.

Oleksandr Byelkin added a comment - 2022-04-14 11:10

The second test suite also repeatable on 10.2 (test was made from 10.6 so I had doubts) and exploit the "deafult" Item directly.

Oleksandr Byelkin added a comment - 2022-04-14 11:53

```
commit bf399cac92f8675bbca5647a6127a1dceff64a44 (HEAD -> bb-10.2-MDEV-26423, o
Author: Oleksandr Byelkin <sanja@mariadb.com>
Date:   Thu Apr 14 13:51:46 2022 +0200

    MDEV-26423 MariaDB server crash in Create_tmp_table::finalize

    Removed prohibition of creating temporary field of Item_default_value
    (added by mistake by 1d9b043a1f5db7ff229d5200652cff7a78ea6266 fix of
    MDEV-10780 and MDEV-11265).
```

Alexander Barkov added a comment - 2022-04-15 13:11

The patch looks OK to push for me. Just one thing, the version number is wrong:

+--echo #
+--echo # End of 1.2 tests
+--echo #

I guess it should be "End of 10.2 tests"

People

Assignee:

Oleksandr Byelkin

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

Dates

Created:

2021-08-19 03:15

Updated:

2022-04-15 15:15

Resolved:

2022-04-15 15:15

Git Integration

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