MariaDB Server MDEV-28082

Crash when using HAVING with IS NULL predicate in an equality

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Duplicate
Affects Version/s:	10.9.0, 10.4, 10.5, 10.6, 10.7, 10.8
Fix Version/s:	10.4.25, 10.5.16, 10.6.8, 10.7.4
Component/s:	Optimizer
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 ( v4 INT , v3 CHAR ( 127 ) NOT NULL , v2 INT , v1 INT NOT NULL ) ;
SELECT * FROM v0 GROUP BY TRUE HAVING v4 = (v1 IS NULL) ;
```

report:

```
Thread pointer: 0x7fc308000c58
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 = 0x7fc3ac1fce30 thread_stack 0x49000
mysys/stacktrace.c:212(my_print_stacktrace)[0xe12bae]
sql/signal_handler.cc:226(handle_fatal_signal)[0x973f04]

sigaction.c:0(__restore_rt)[0x7fc3c4abc3c0]
sql/item_cmpfunc.h:2728(Item_func_isnull::arg_is_datetime_notnull_field())[0x9b
sql/item.h:5311(Used_tables_and_const_cache::used_tables_and_const_cache_join(I
??:0(eliminate_item_equal(THD*, Item*, COND_EQUAL*, Item_equal*))[0x7ad9f9]
sql/sql_select.cc:16391(substitute_for_best_equal_field(THD*, st_join_table*, I
sql/sql_select.cc:2612(JOIN::optimize_stage2())[0x78b60f]
sql/sql_select.cc:2492(JOIN::optimize_inner())[0x7922a2]
??:0(JOIN::optimize())[0x78af00]
```

```
sql/sql_select.cc:4993(mysql_select(THD*, TABLE_LIST*, List<Item>&, Item*, unsi
select_lex*))[0x785468]
sql/sql_select.cc:543(handle_select(THD*, LEX*, select_result*, unsigned long))
```

Issue Links

duplicates

MDEV-26402 A SEGV in Item_field::used_tables/update_depend_map_for... CLOSED

links to

CVE-2022-27446

Activity

Alice Sherepa added a comment - 2022-03-18 15:22

Thank you for the report!
It is reproducible on 10.4-10.9, workaround-set
optimizer_switch='condition_pushdown_from_having=off'

```
set optimizer_switch='condition_pushdown_from_having=on';

CREATE TABLE t1 (a int, b int NOT NULL) ;
select a,b from t1 group by a having a = (b is null) ;
```

with MyISAM:

10.4 069139a549a62f26d566c1ae

```
Version: '10.4.25-MariaDB-debug-log'
220318 15:54:37 [ERROR] mysqld got signal 11 ;



sigaction.c:0(__restore_rt)[0x7fc64dbd03c0]
sql/item.cc:6489(Item_field::make_send_field(THD*, Send_field*))[0x5606236
sql/field.cc:11218(Send_field::Send_field(THD*, Item*))[0x56062355bfe6]
sql/protocol.cc:997(Protocol_text::store_field_metadata(THD*, Item*, unsig
sql/protocol.cc:914(Protocol::send_result_set_metadata(List<Item>*, unsign
sql/sql_class.cc:3068(select_send::send_result_set_metadata(List<Item>&, u
sql/sql_select.cc:14485(return_zero_rows(JOIN*, select_result*, List<TABLE
sql/sql_select.cc:4465(JOIN::exec_inner())[0x560622ec978b]
sql/sql_select.cc:4325(JOIN::exec())[0x560622ec79da]
```

10.4 069139a549a62f26d566c1ae

```
sql/sql_select.cc:4765(mysql_select(THD*, TABLE_LIST*, unsigned int, List<
sql/sql_select.cc:436(handle_select(THD*, LEX*, select_result*, unsigned l
sql/sql_parse.cc:6449(execute_sqlcom_select(THD*, TABLE_LIST*))[0x560622e0
sql/sql_parse.cc:3963(mysql_execute_command(THD*))[0x560622df8b3e]
```

With INNODB:

10.4 069139a549a62f26d566c1ae

```
Version: '10.4.25-MariaDB-debug-log'
220318 16:16:46 [ERROR] mysqld got signal 11 ;

sql/signal_handler.cc:222(handle_fatal_signal)[0x5643fe46d873]


sigaction.c:0(__restore_rt)[0x7f19702fa3c0]
sql/item_cmpfunc.h:2568(Item_func_isnull::arg_is_datetime_notnull_field())
sql/item_cmpfunc.h:2578(Item_func_isnull::update_used_tables())[0x5643fe58
sql/item.h:5141(Used_tables_and_const_cache::used_tables_and_const_cache_u
sql/item.h:5151(Used_tables_and_const_cache::used_tables_and_const_cache_u
sql/item_func.h:161(Item_func::update_used_tables())[0x5643fdb6da78]
sql/sql_select.cc:15873(eliminate_item_equal(THD*, Item*, COND_EQUAL*, Ite
sql/sql_select.cc:16047(substitute_for_best_equal_field(THD*, st_join_tabl
sql/sql_select.cc:2461(JOIN::optimize_stage2())[0x5643fdd8b67e]
sql/sql_select.cc:2342(JOIN::optimize_inner())[0x5643fdd89fc2]
sql/sql_select.cc:1659(JOIN::optimize())[0x5643fdd82bda]
sql/sql_select.cc:4749(mysql_select(THD*, TABLE_LIST*, unsigned int, List<
```

Igor Babaev added a comment - 2022-04-28 04:12

This bug has been actually fixed by the patch for ~~MDEV-26402~~. Only a test case of ~~MDEV-28082~~ will be added to 10.4.

Igor Babaev added a comment - 2022-04-29 17:04

Here's a more general test case that conforms to the Standard SQL.

```sql
CREATE TABLE t1 (a int, b int NOT NULL) ;
INSERT INTO t1 VALUES (1,10), (0,11), (0,11), (1,10);

SELECT a,b FROM t1 GROUP BY a,b HAVING a = (b IS NULL) ;

DROP TABLE t1;
```

Yet execution of the SELECT in this test case causes a crash of the server earlier:

```
sql/signal_handler.cc:222(handle_fatal_signal)[0x55c52ade0510]
/lib64/libpthread.so.0(+0xf890)[0x7fda531ff890]
sql/item.cc:3404(Item_field::used_tables() const)[0x55c52ae0b559]
sql/sql_select.cc:14135(update_depend_map_for_order(JOIN*, st_order*))[0x55c52
sql/sql_select.cc:14243(remove_const(JOIN*, st_order*, Item*, bool, bool*))[0x
sql/sql_select.cc:2299(JOIN::optimize_inner())[0x55c52aaedf1a]
sql/sql_select.cc:1661(JOIN::optimize())[0x55c52aaeb8ad]
sql/sql_select.cc:4752(mysql_select(THD*, TABLE_LIST*, unsigned int, List<Item
sql/sql_select.cc:448(handle_select(THD*, LEX*, select_result*, unsigned long)
sql/sql_parse.cc:6465(execute_sqlcom_select(THD*, TABLE_LIST*))[0x55c52aaab721
sql/sql_parse.cc:3979(mysql_execute_command(THD*))[0x55c52aaa21c9]
sql/sql_parse.cc:8011(mysql_parse(THD*, char*, unsigned int, Parser_state*, bo
sql/sql_parse.cc:1876(dispatch_command(enum_server_command, THD*, char*, unsig
sql/sql_parse.cc:1379(do_command(THD*))[0x55c52aa9a489]
sql/sql_connect.cc:1420(do_handle_one_connection(CONNECT*))[0x55c52ac2c1a1]
sql/sql_connect.cc:1317(handle_one_connection)[0x55c52ac2be4b]
perfschema/pfs.cc:1871(pfs_spawn_thread)[0x55c52b17ea81]
/lib64/libpthread.so.0(+0x80a4)[0x7fda531f80a4]
/lib64/libc.so.6(clone+0x6d)[0x7fda5263004d]
```

Igor Babaev added a comment - 2022-04-29 23:45

A test case for this bug was pushed into 10.4

People

Assignee:

Igor Babaev

Reporter:

Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

Dates

Created:

2022-03-16 09:19

Updated:

2022-05-03 09:57

Resolved:

2022-04-29 14:43

Git Integration

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