MariaDB Server MDEV-28080

Crash when using HAVING with NOT EXIST 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 v2 ( v3 INT ( 29 ) ) ;
SELECT ( 'x' ) FROM v2 GROUP BY v3 HAVING v3 = ( NOT EXISTS ( SELECT * WHERE 'x' )
```

report (compiled with ASAN):

```
Thread pointer: 0x7f0dac000c58
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 = 0x7f0e10057e30 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)[0x7f0e1b8b53c0]
sql/item_subselect.cc:4026(subselect_single_select_engine::exec())[0xa36cdc]
sql/item_subselect.cc:858(Item_subselect::exec())[0xa2e4bc]
sql/item_subselect.cc:1872(Item_exists_subselect::val_bool())[0xa30a1e]
sql/item_cmpfunc.cc:202(Item_func_not::val_int())[0x9a6739]
sql/sql_type.cc:8716(Type_handler_int_result::Item_eq_value(THD*, Type_cmp_attr
sql/item_cmpfunc.cc:6746(Item_equal::add_const(THD*, Item*))[0x9b79d8]
??:0(Item_equal::merge_with_check(THD*, Item_equal*, bool))[0x9b7d7b]
```

```
sql/sql_list.h:429(base_list_iterator::next())[0x7aec59]
sql/field.h:429(Context)[0x899f87]
??:0(JOIN::optimize_inner())[0x79112c]
```

Issue Links

duplicates

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

relates to

MDEV-25084 Assertion `fixed' or Assertion `i->is_fixed()' fail with conditi... CONFIRMED

links to

CVE-2022-27444

Activity

Alice Sherepa added a comment - 2022-03-18 11:58 - edited

Thanks! I repeated on 10.4-10.8, a temporary workaround - optimizer_switch='condition_pushdown_from_having=off';

```
set optimizer_switch='condition_pushdown_from_having=on';
CREATE TABLE t1 (a int);
SELECT 1 FROM t1 GROUP BY a HAVING a= (NOT EXISTS (SELECT 1));
```

10.4 069139a549a62f26d566c1ae

```
Version: '10.4.25-MariaDB-debug-log'
mysqld: /10.4/src/sql/item_subselect.cc:1799: virtual bool Item_exists_sub
220318  9:59:21 [ERROR] mysqld got signal 6 ;

Server version: 10.4.25-MariaDB-debug-log

sql/item_subselect.cc:1800(Item_exists_subselect::val_bool())[0x556271a47c


sql/item_cmpfunc.cc:200(Item_func_not::val_int())[0x5562718d37cc]
sql/sql_type.cc:8270(Type_handler_int_result::Item_eq_value(THD*, Type_cmp
sql/item_cmpfunc.cc:6653(Item_equal::add_const(THD*, Item*))[0x5562719154b
sql/item_cmpfunc.cc:6779(Item_equal::merge_with_check(THD*, Item_equal*, b
sql/sql_select.cc:17242(propagate_new_equalities(THD*, Item*, List<Item_eq
sql/opt_subselect.cc:6012(and_new_conditions_to_optimized_cond(THD*, Item*
```

10.4 969139a549a62f26d566c1ae

```
sql/sql_select.cc:2091(JOIN::optimize_inner())[0x5562711299ac]
sql/sql_select.cc:1659(JOIN::optimize())[0x556271124bda]
sql/sql_select.cc:4749(mysql_select(THD*, TABLE_LIST*, unsigned int, List<
```

on 10.6+ assertion was renamed -10.6/src/sql/item_subselect.cc:1872: virtual bool Item_exists_subselect::val_bool(): Assertion `fixed()' failed.

Igor Babaev added a comment - 2022-04-28 04:11

This bug has been actually fixed by the patch for ~~MDEV-26402~~. Only a test case of ~~MDEV-28080~~ will be added to 10.4.

Igor Babaev added a comment - 2022-04-29 16:20

Here's a more general test case that causes the same crash:

```
CREATE TABLE t1 (a int);
CREATE TABLE t2 (b int);
INSERT INTO t1 VALUES (0), (1), (1), (0);
INSERT INTO t2 VALUES (3), (7);

SELECT a FROM t1
  GROUP BY a HAVING a= (NOT EXISTS (SELECT b FROM t2 WHERE b = 1));
SELECT a FROM t1
  GROUP BY a HAVING a= (NOT EXISTS (SELECT b FROM t2 WHERE b = 7));

DROP TABLE t1, t2;
```

Igor Babaev added a comment - 2022-04-29 23:44

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:

4 Start watching this issue

Dates

Created:

2022-03-16 09:13

Updated:

2022-05-03 06:46

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.