





MariaDB Server

MDEV-26412

Server crash in Item_field::fix_outer_field for INSERT SELECT

▼ Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Major
Resolution:	Fixed
Affects Version/s:	10.4, 10.5, 10.6, 10.7, 10.8
Fix Version/s:	10.4.25 , 10.5.16 , 10.6.8 , (2)
Component/s:	Data Manipulation - Insert
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 ( v1 BIGINT ( 67 ) NOT NULL ) ;  
CREATE TABLE v2 ( v4 INT , v3 INT NOT NULL UNIQUE KEY CHECK ( -128 | ( str_to_date  
DROP FUNCTION IF EXISTS v0 ;  
INSERT INTO v0 SELECT DISTINCT * FROM v0 FULL JOIN v2 ON ( SELECT v0 . v1 ) ;
```

Crash Log:

```
Version: '10.7.0-MariaDB' socket: '/tmp/18.socket' port: 10018 Source distri  
210816 15:33:24 [ERROR] mysqld got signal 11 ;
```

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
```



▼ Issue Links

is duplicated by

 [MDEV-26214](#) INSERT from SELECT crashes server on error missing column.  **CLOSED**

relates to

 [MDEV-29088](#) Server crash upon CREATE VIEW with unknown column in ...  **CLOSED**


 [MDEV-25346](#) Server crashes in Item_field::fix_outer_field upon subquery ...  **IN PROGRESS**

 [MDEV-28578](#) Server crashes in Item_field::fix_outer_field after CREATE SE...  **CLOSED**

links to

 [CVE-2022-32086](#)

▼ Activity

▼  [Alice Sherepa](#) added a comment - 2021-08-27 08:49

Thank you!

I repeated the crash on 10.4-10.6, 10.2-10.3 returns error -Unknown column 't1.i' in 'field list'

```
CREATE TABLE t1 (i int) ;
CREATE TABLE t2 (j int) ;
INSERT INTO t1 SELECT * FROM t1 FULL JOIN t2 ON (SELECT t1.i);
```


10.4 dc6bc85cd29586631d

Version: '10.4.22-MariaDB-debug-log'

210827 10:46:46 [ERROR] mysqld got signal 11 ;

```
sql/signal_handler.cc:222(handle_fatal_signal)[0x55dd5eb0bfb3]
sigaction.c:0(__restore_rt)[0x7fcd62ddc3c0]
sql/item.cc:5457(Item_field::fix_outer_field(THD*, Field**, Item**))[0x55d
sql/item.cc:5872(Item_field::fix_fields(THD*, Item**))[0x55dd5eb8d319]
sql/item.h:964(Item::fix_fields_if_needed(THD*, Item**))[0x55dd5e06b969]
```

```
1014 de6bc85c129586631d1 sql/item.h:968(Item::fix_fields_if_needed_for_scalar(THD*, Item**))[0x55dd
sql/sql_base.cc:7723(setup_fields(THD*, Bounds_checked_array<Item*>, List<
sql/sql_select.cc:1276(JOIN::prepare(TABLE_LIST*, unsigned int, Item*, uns
sql/item_subselect.cc:3825(subselect_single_select_engine::prepare(THD*))[
sql/item_subselect.cc:289(Item_subselect::fix_fields(THD*, Item**))[0x55dd
sql/item.h:964(Item::fix_fields_if_needed(THD*, Item**))[0x55dd5e06b969]
sql/item.h:968(Item::fix_fields_if_needed_for_scalar(THD*, Item**))[0x55dd
sql/item.h:973(Item::fix_fields_if_needed_for_bool(THD*, Item**))[0x55dd5e
```

✓  Oleksandr Byelkin added a comment - 2022-04-27 13:18


OK to push

✓  Igor Babaev added a comment - 2022-04-28 05:12


A fix for this bug was pushed into 10.4

▼ People

Assignee:

 Igor Babaev

Reporter:

 yaoguang

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

▼ Dates

Created:

2021-08-19 02:54

Updated:

2022-07-13 18:14

Resolved:

2022-04-28 05:12

▼ Git Integration

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