





MariaDB Server

MDEV-26047

MariaDB server crash at Item_subselect::init_expr_cache_tracker

Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Blocker
Resolution:	Fixed
Affects Version/s:	10.6.1, 10.5.11, 10.2, 10.3, 10.4, 10.5, 10.6
Fix Version/s:	10.2.44 , 10.3.35 , 10.4.25 , (4)
Component/s:	Optimizer
Labels:	crash regression
Environment:	Linux 5.4.0-39-generic #43-Ubuntu SMP Fri Jun 19 10:28:31 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

Description

Steps to reproduce:

```
CREATE TABLE v0 ( v1 INT PRIMARY KEY ) ;
INSERT INTO v0 VALUES ( ( ( 23695630.000000 ) ) NOT IN ( SELECT DISTINCT - ( 89 IN
CREATE TABLE v3 ( v4 INTEGER , v5 INT PRIMARY KEY , v6 VARCHAR ( 24 ) , v7 INT , v
INSERT INTO v3 ( v5 ) VALUES ( ( ( - ( ( 'x' IS NOT NULL ) ) ) ) ) , ( 55 BETWEEN
```

Backtrace:



Core was generated by `/home/supersix/fuzz/security/MariaDB/install/bin/mysqld --defaults-file=/home/s'.

```
Program terminated with signal SIGSEGV, Segmentation fault.
#0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0xb)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
[Current thread is 1 (Thread 0x7f0f26251300 (LWP 1437547))]
gdb-peda$ #0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0xb)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
#1  0x0000559d3cfff698f in my_write_core (sig=sig@entry=0xb)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/mysys/stacktrace.c:4
#2  0x0000559d3ba63583 in handle_fatal_signal (sig=<optimized out>)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/signal_handler.c
```



```
#3 <signal handler called>
#4 0x0000559d3be106ea in Item_subselect::init_expr_cache_tracker (
    this=0x6290021eddb8, thd=<optimized out>)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/sql_lex.h:982
#5 0x0000559d3be108df in Item_singlerow_subselect::expr_cache_insert_transform
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/item_subselect.c
#6 0x0000559d3bab3024 in Item::transform (this=<optimized out>,
    thd=<optimized out>, transformer=<optimized out>, arg=<optimized out>)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/item.cc:610
```


▼ Issue Links

causes

 [MDEV-28437](#) Assertion '!eliminated' failed in Item_subselect::exec  **CLOSED**

is duplicated by

 [MDEV-26164](#) crash in Item_subselect::init_expr_cache_tracker  **CLOSED**

 [MDEV-26428](#) MariaDB Server SEGV issue  **CLOSED**

relates to

 [MDEV-24925](#) Server crashes in Item_subselect::init_expr_cache_tracker  **CLOSED**


links to

 [CVE-2022-27384](#)


[Show 1 more links](#) (1 links to)

▼ Activity

10 older comments

▼  [Sergei Petrunia](#) added a comment - 2022-04-22 17:27

A patch: <https://github.com/MariaDB/server/commit/c01ee954bf3b10fef85af7b8c77d319ff7bd6b61>

▼  [Sergei Petrunia](#) added a comment - 2022-04-22 17:28


Note that this patch doesn't fix [MDEV-27957](#). for that MDEV, a crash becomes a memory leak (one can see it reported by e.g. my_malloc)

▼  [Sergei Petrunia](#) added a comment - 2022-04-22 17:28 - **edited**

Oleksandr Byelkin please review

- ▼  Sergei Petrunia added a comment - 2022-04-22 18:01

Note: for unused fields in select lists, we had intent to fix this in the future versions: [MDEV-27201](#).

- ▼  Oleksandr Byelkin added a comment - 2022-04-24 09:52


OK to push

▼ People

Assignee:

 Sergei Petrunia

Reporter:

 yaoguang

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

▼ Dates

Created:

2021-06-30 06:35


Updated:

2022-07-02 07:49

Resolved:

2022-04-26 12:55

▼ Git Integration

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