

# MariaDB server crash at Item\_subselect::init\_expr\_cache\_tracker

#### Details

Type:

Status: **CLOSED** (View Workflow)

Bug

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

(crash) (regression) Labels:

**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

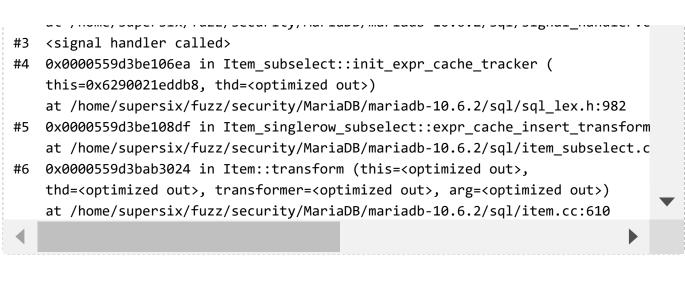
## Steps to reproduce:

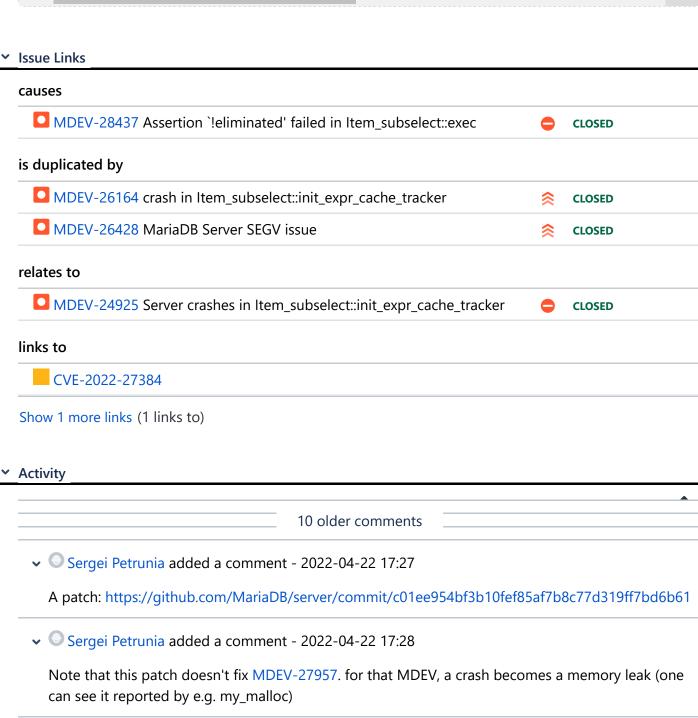
```
CREATE TABLE v0 ( v1 INT PRIMARY KEY );
INSERT INTO v0 VALUES ( ( ( 23695630.000000 ) ) NOT IN ( SELECT DISTINCT - ( 89 IN
CREATE TABLE v3 ( v4 INTEGER , v5 INT PRIMARY KEY , v6 VARCHAR ( 24 ) , v7 INT , v
INSERT INTO v3 ( v5 ) VALUES ( ( ( - ( ( 'x' IS NOT NULL ) ) ) ) , ( 55 BETWEEN
```

#### Backtrace:

Core was generated by `/home/supersix/fuzz/security/MariaDB/install/bin/mysqld --defaultsfile=/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 0x0000559d3cff698f 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
```





✓ Sergei Petrunia added a comment - 2022-04-22 17:28 - edited

✓ 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.
Note. for difused fields in select lists, we flad liftent to fix this in the fatare 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.