





MariaDB Server

MDEV-26431

# MariaDB Server use-after-poison

## Details

Type:	 Bug
Status:	CLOSED ( <a href="#">View Workflow</a> )
Priority:	 Major
Resolution:	Duplicate
Affects Version/s:	10.7.0
Fix Version/s:	<a href="#">10.3.36</a> , <a href="#">10.4.26</a> , <a href="#">10.5.17</a> , (3)
Component/s:	N/A
Labels:	None
Environment:	Linux version 5.13.0-1-MANJARO ( <a href="#">builduser@LEGION</a> ) (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

step to reproduce:

```
CREATE TABLE v0 ( v2 BIGINT , v1 BIGINT ) ENGINE = MEMORY ROW_FORMAT = COMPRESSED A
START TRANSACTION ;
SELECT instr ( v1 , DES_ENCRYPT ( 'x' REGEXP 'x' , 'x' ) ) BETWEEN v3 AND -1 FROM
SELECT DISTINCT v2 IN ( COLLATION ( AVG ( 'x' ) ) + -128 , 'x' , 'x' ) FROM v0 WHE
UPDATE v0 SET v2 = v3 + 69 ;
INSERT INTO v0 ( ) SELECT v1 , v1 FROM v0 ;
```



asan report:

```
=====
==2933067==ERROR: AddressSanitizer: use-after-poison on address 0x6290000a6080
WRITE of size 944 at 0x6290000a6080 thread T14
#0 0x7fb1687ce7b6 in __interceptor_memset /build/gcc/src/gcc/libsanitizer/s
#1 0x55c6bfcc41e9 in JOIN::make_aggr_tables_info() /experiment/mariadb-serv
#2 0x55c6bfcf2e71 in JOIN::optimize_stage2() /experiment/mariadb-server/sql
#3 0x55c6bfcfcd06 in JOIN::optimize_inner() /experiment/mariadb-server/sql/
#4 0x55c6bfcfe7b0 in JOIN::optimize() /experiment/mariadb-server/sql/sql_se
#5 0x55c6bfcfea0d in mysql_select(THD*, TABLE_LIST*, List<Item>&, Item*, un
#6 0x55c6bfd00654 in handle_select(THD*, LEX*, select_result*, unsigned lon
#7 0x55c6bfb43d7c in execute_sqlcom_select /experiment/mariadb-server/sql/s
#8 0x55c6bfb6d420 in mysql_execute_command(THD*, bool) /experiment/mariadb-
```

```
#9 0x55c6bfb725a0 in mysql_parse(THD*, char*, unsigned int, Parser_state*)
#10 0x55c6bfb7860b in dispatch_command(enum_server_command, THD*, char*, un
#11 0x55c6bfb7d73c in do_command(THD*, bool) /experiment/mariadb-server/sql
#12 0x55c6bff38e56 in do_handle_one_connection(CONNECT*, bool) /experiment/
#13 0x55c6bff3933c in handle_one_connection /experiment/mariadb-server/sql/
#14 0x55c6c09c9c2b in pfs_spawn_thread /experiment/mariadb-server/storage/p
```

## ▼ Issue Links


### duplicates

 [MDEV-23809](#) Server crash in JOIN\_CACHE::free or in copy\_fields, ASAN u...  **CLOSED**

### links to

 [CVE-2022-32091](#)

## ▼ Activity


▼  [Alice Sherepa](#) added a comment - 2021-08-27 14:17

Thanks!


This is the same as [MDEV-23809](#)

## ▼ People

Assignee:

 Unassigned

Reporter:

 [Jingzhou Fu](#)

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

## ▼ Dates

Created:

2021-08-19 04:25

Updated:

2022-08-05 07:38

Resolved:

2021-08-27 14:17

#### ▼ Git Integration

---

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