





MariaDB Server

MDEV-26354

## MariaDB server crash in Field::set\_default - ASAN use after free in Item\_args::walk\_arg

### Details

Type:  Bug  
Status: **CLOSED** ([View Workflow](#))  
Priority:  Critical  
Resolution: Duplicate  
Affects Version/s: 10.5.13, 10.6.5, 10.2, 10.3, 10.4  
Fix Version/s: [N/A](#)  
Component/s: [N/A](#)  
Labels: [crash](#)  
Environment: Linux x64

### Description

step to reproduce:

```
CREATE TEMPORARY TABLE v0 ( v2 LONG VARBINARY DEFAULT ( USER ( ) REGEXP 'x' IS NULL  
INSERT IGNORE INTO v0 VALUES ( v1 , 'x' , ( CONVERT ( v2 * ( 47347653.000000 - v1 )  
ALTER TABLE v0 CONVERT TO CHARSET BINARY ;  
INSERT HIGH_PRIORITY INTO v0 SELECT * FROM v0 USE INDEX FOR JOIN ( ) GROUP BY v1 ,  
INSERT INTO v0 SELECT SQL_CALC_FOUND_ROWS * FROM v0 WHERE v2 SOUNDS LIKE CURRENT_US
```

asan report:

Version: '10.6.5-MariaDB' socket: '/tmp/mysql\_mar.sock' port: 3309 Source distribution

=====

==1434754==ERROR: AddressSanitizer: use-after-poison on address 0x62b00007aec8 at pc

0x55bf6a845200 bp 0x7fd6c0eb93c0 sp 0x7fd6c0eb93b0

READ of size 8 at 0x62b00007aec8 thread T23

#0 0x55bf6a8451ff in Item\_args::walk\_args(bool (Item::)(void), bool, void\*)

MariaDB/server/sql/item.h:2742

#1 0x55bf6a8451ff in Item\_func\_or\_sum::walk(bool (Item::)(void), bool, void\*)

MariaDB/server/sql/item.h:5434

#2 0x55bf6a8450e1 in Item\_args::walk\_args(bool (Item::)(void), bool, void\*)

MariaDB/server/sql/item.h:2742

#3 0x55bf6a8450e1 in Item\_func\_or\_sum::walk(bool (Item::)(void), bool, void\*)

MariaDB/server/sql/item.h:5434

#4 0x55bf6a8450e1 in Item\_args::walk\_args(bool (Item::)(void), bool, void\*)

MariaDB/server/sql/item.h:2742  
#5 0x55bf6a8450e1 in Item\_func\_or\_sum::walk(bool (Item::)(**void**), bool, void\*)  
MariaDB/server/sql/item.h:5434  
#6 0x55bf6a8450e1 in Item\_args::walk\_args(bool (Item::)(**void**), bool, void\*)  
MariaDB/server/sql/item.h:2742  
#7 0x55bf6a8450e1 in Item\_func\_or\_sum::walk(bool (Item::)(**void**), bool, void\*)  
MariaDB/server/sql/item.h:5434  
#8 0x55bf6ad6beb9 in fix\_session\_vcol\_expr(THD\*, Virtual\_column\_info\*)  
MariaDB/server/sql/table.cc:3614  
#9 0x55bf6ad6beb9 in fix\_session\_vcol\_expr(THD\*, Virtual\_column\_info\*)  
MariaDB/server/sql/table.cc:3608  
#10 0x55bf6a7c973e in TABLE::fix\_vcol\_exprs(THD\*) MariaDB/server/sql/sql\_base.cc:5434  
#11 0x55bf6a7c973e in TABLE::fix\_vcol\_exprs(THD\*) MariaDB/server/sql/sql\_base.cc:5426  
#12 0x55bf6a7ca468 in fix\_all\_session\_vcol\_exprs MariaDB/server/sql/sql\_base.cc:5465  
#13 0x55bf6a7ca468 in lock\_tables(THD\*, TABLE\_LIST\*, unsigned int, unsigned int)  
MariaDB/server/sql/sql\_base.cc:5649  
#14 0x55bf6a7d0ba2 in open\_and\_lock\_tables(THD\*, DDL\_options\_st const&, TABLE\_LIST\*, bool, unsigned int, Prelocking\_strategy\*) MariaDB/server/sql/sql\_base.cc:5261  
#15 0x55bf6a9baf70 in open\_and\_lock\_tables(THD\*, TABLE\_LIST\*, bool, unsigned int)  
MariaDB/server/sql/sql\_base.h:509  
#16 0x55bf6a9a8388 in mysql\_execute\_command(THD\*, bool) MariaDB/server/sql/sql\_parse.cc:4649  
#17 0x55bf6a966684 in mysql\_parse(THD\*, char\*, unsigned int, Parser\_state\*)  
MariaDB/server/sql/sql\_parse.cc:8030  
#18 0x55bf6a99c0b3 in dispatch\_command(enum\_server\_command, THD\*, char\*, unsigned int, bool)  
MariaDB/server/sql/sql\_parse.cc:1896  
#19 0x55bf6a9a1513 in do\_command(THD\*, bool) MariaDB/server/sql/sql\_parse.cc:1404  
#20 0x55bf6ae636fc in do\_handle\_one\_connection(CONNECT\*, bool)  
MariaDB/server/sql/sql\_connect.cc:1418  
#21 0x55bf6ae64e56 in handle\_one\_connection MariaDB/server/sql/sql\_connect.cc:1312  
#22 0x55bf6bcb0d2f in pfs\_spawn\_thread MariaDB/server/storage/perfschema/pfs.cc:2201  
#23 0x7fd6e0503608 in start\_thread /build/glibc-ZN95T4/glibc-2.31/nptl/pthread\_create.c:477  
#24 0x7fd6e00d7292 in \_\_clone (/lib/x86\_64-linux-gnu/libc.so.6+0x122292)

0x62b00007aec8 is located 15560 bytes inside of 24624-byte region [0x62b000077200,0x62b00007d230) allocated by thread T23 here:

#0 0x7fd6e0a8ebc8 in malloc (/lib/x86\_64-linux-gnu/libasan.so.5+0x10dbc8)  
#1 0x55bf6c83cc1c in my\_malloc MariaDB/server/mysys/my\_malloc.c:90  
#2 0x55bf6c8238c8 in reset\_root\_defaults MariaDB/server/mysys/my\_alloc.c:148  
#3 0x55bf6a813773 in THD::init\_for\_queries() MariaDB/server/sql/sql\_class.cc:1406  
#4 0x55bf6ae611ea in prepare\_new\_connection\_state(THD\*) MariaDB/server/sql/sql\_connect.cc:1240  
#5 0x55bf6ae61efa in thd\_prepare\_connection(THD\*) MariaDB/server/sql/sql\_connect.cc:1333  
#6 0x55bf6ae61efa in thd\_prepare\_connection(THD\*) MariaDB/server/sql/sql\_connect.cc:1322  
#7 0x55bf6ae63663 in do\_handle\_one\_connection(CONNECT\*, bool)  
MariaDB/server/sql/sql\_connect.cc:1408  
#8 0x55bf6ae64e56 in handle\_one\_connection MariaDB/server/sql/sql\_connect.cc:1312  
#9 0x55bf6bcb0d2f in pfs\_spawn\_thread MariaDB/server/storage/perfschema/pfs.cc:2201  
#10 0x7fd6e0503608 in start\_thread /build/glibc-ZN95T4/glibc-2.31/nptl/pthread\_create.c:477

Thread T23 created by T0 here:

#0 0x7fd6e09bb805 in pthread\_create (/lib/x86\_64-linux-gnu/libasan.so.5+0x3a805)  
#1 0x55bf6bcb0fe2 in my\_thread\_create MariaDB/server/storage/perfschema/my\_thread.h:48  
#2 0x55bf6bcb0fe2 in pfs\_spawn\_thread\_v1 MariaDB/server/storage/perfschema/pfs.cc:2252  
#3 0x55bf6a635b48 in inline\_mysql\_thread\_create  
MariaDB/server/include/mysql/psi/mysql\_thread.h:1139  
#4 0x55bf6a635b48 in create\_thread\_to\_handle\_connection(CONNECT\*)  
MariaDB/server/sql/mysqld.cc:5922  
#5 0x55bf6a645235 in handle\_accepted\_socket(st\_mysql\_socket, st\_mysql\_socket)  
MariaDB/server/sql/mysqld.cc:6043  
#6 0x55bf6a64600e in handle\_connections\_sockets() MariaDB/server/sql/mysqld.cc:6167  
#7 0x55bf6a64819b in mysqld\_main(int, char\*\*) MariaDB/server/sql/mysqld.cc:5817  
#8 0x7fd6dffdc0b2 in \_\_libc\_start\_main (/lib/x86\_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: use-after-poison MariaDB/server/sql/item.h:2742 in  
Item\_args::walk\_args(bool (Item::)(void), bool, void\*)

Shadow bytes around the buggy address:

0x0c5680007580: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c5680007590: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c56800075a0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c56800075b0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c56800075c0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
=>0x0c56800075d0: f7 f7 f7 f7 f7 f7 f7 f7 f7[f7]f7 f7 f7 f7 f7  
0x0c56800075e0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c56800075f0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c5680007600: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c5680007610: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7  
0x0c5680007620: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7

Shadow byte legend (one shadow byte represents 8 application bytes):

Addressable: 00

Partially addressable: 01 02 03 04 05 06 07

Heap left redzone: fa

Freed heap region: fd

Stack left redzone: f1

Stack mid redzone: f2

Stack right redzone: f3

Stack after return: f5

Stack use after scope: f8

Global redzone: f9

Global init order: f6

Poisoned by user: f7

Container overflow: fc

Array cookie: ac

Intra object redzone: bb

ASan internal: fe

Left alloca redzone: ca

Right alloca redzone: cb

Shadow gap: cc  
==1434754==ABORTING

## ▼ Issue Links

### duplicates

 [MDEV-26437](#) Server crashes in Item\_args::walk\_args

 **CLOSED**

### links to

 [CVE-2022-27376](#)

## ▼ Activity



▼  [Daniel Black](#) added a comment - 2021-08-13 08:28

Confirmed:

#### 10.5.13-0268b871228-debug


```
2021-08-13 18:25:34 0 [Note] /home/dan/repos/build-mariadb-server-10.5-asa
Version: '10.5.13-MariaDB-debug' socket: '/tmp/build-mariadb-server-10.5-
[New Thread 0x7fffccf80640 (LWP 791170)]
```

```
=====
```

```
==791142==ERROR: AddressSanitizer: use-after-poison on address 0x62b0000a5
READ of size 8 at 0x62b0000a5188 thread T25
```

```
[Detaching after fork from child process 791183]
```

```
#0 0xadb2ac in Item_args::walk_args(bool (Item::*)(void*), bool, void*
#1 0xad8424 in Item_func_or_sum::walk(bool (Item::*)(void*), bool, voi
#2 0xadb2f9 in Item_args::walk_args(bool (Item::*)(void*), bool, void*
#3 0xad8424 in Item_func_or_sum::walk(bool (Item::*)(void*), bool, voi
#4 0xadb2f9 in Item_args::walk_args(bool (Item::*)(void*), bool, void*
#5 0xad8424 in Item_func_or_sum::walk(bool (Item::*)(void*), bool, voi
#6 0xadb2f9 in Item_args::walk_args(bool (Item::*)(void*), bool, void*
#7 0xad8424 in Item_func_or_sum::walk(bool (Item::*)(void*), bool, voi
#8 0x10cb223 in fix_session_vcol_expr(THD*, Virtual_column_info*) /hom
#9 0xaab9a9 in TABLE::fix_vcol_exprs(THD*) /home/dan/repos/mariadb-ser
#10 0xaac572 in fix all session vcol exprs(THD*. TABLE LIST*) /home/da
```


▼  [Alice Sherepa](#) added a comment - 2021-08-25 12:07

Thanks!


This is the same bug as [MDEV-26437](#)

## ▼ People

Assignee:

 Unassigned

Reporter:

 yaoguang

Votes:

0 Vote for this issue

Watchers:

4 Start watching this issue

#### ▼ Dates

---

Created:

2021-08-13 07:22

Updated:

2022-04-27 16:22

Resolved:

2021-08-25 12:07

#### ▼ Git Integration

---



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