





MariaDB Server

MDEV-26353

MariaDB server crash in Arg_comparator::compare_real_fixed

Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Major
Resolution:	Duplicate
Affects Version/s:	10.6.2, 10.5.13, 10.2, 10.3, (3)
Fix Version/s:	N/A
Component/s:	Data types
Labels:	None
Environment:	Linux x64

Description

Reported by:

Yaoguang Chen of Ant Security Light-Year Lab

Steps to reproduce:

```
CREATE TEMPORARY TABLE v0 ( v4 SMALLINT , v3 TINYINT , v2 NCHAR BINARY GENERATED ALWAYS AS (SELECT CONVERT ( CHAR ( 'x' IS FALSE ) * DEFAULT ( v2 ) * 'x' * 62721821.000000 , 10.6.2.000000 ) ) , v1 IN ( 'x' , FALSE ) ) ;
INSERT IGNORE INTO v0 VALUES ( 78470821.000000 , 'x' , -32768 , v1 IN ( 'x' , FALSE ) ) ;
```

backtrace:

```
Core was generated by `/home/supersix/fuzz/security/MariaDB/install_debug/bin/mariadb'
Program terminated with signal SIGABRT, Aborted.
#0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0x6)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
56      ../sysdeps/unix/sysv/linux/pthread_kill.c: No such file or directory.
[Current thread is 1 (Thread 0x7f8010296700 (LWP 1431325))]
gdb-peda$ bt
#0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0x6)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
#1  0x000055ceeec1e94f in my_write_core (sig=sig@entry=0x6)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/mysys/stacktrace.c:4
#2  0x000055cee729d60 in handle_fatal_signal (sig=0x6)
```

```
at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/signal_handler.c
#3 <signal handler called>
#4 __GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:50
#5 0x00007f8010d68859 in __GI_abort () at abort.c:79
#6 0x00007f801113f951 in ?? () from /lib/x86_64-linux-gnu/libstdc++.so.6
#7 0x00007f801114b47c in ?? () from /lib/x86_64-linux-gnu/libstdc++.so.6
```

▼ Issue Links

duplicates

 [MDEV-26437](#) Server crashes in Item_args::walk_args

 **CLOSED**

links to

 [CVE-2022-27379](#)

▼ Activity

▼  [Daniel Black](#) added a comment - 2021-08-13 08:23

Thank you Yaoguang Chen for your bug report.

Can you include the minor version number also in the Affected Versions of your bug report. I'm going off your backtrace as 10.6.2.


My confirmation:

10.5.13-0268b871228-debug-asan

```
2021-08-13 18:14:51 0 [Note] InnoDB: 10.5.13 started; log sequence number
2021-08-13 18:14:51 0 [Note] InnoDB: Loading buffer pool(s) from /tmp/build
2021-08-13 18:14:51 0 [Note] Plugin 'FEEDBACK' is disabled.
2021-08-13 18:14:51 0 [Note] InnoDB: Buffer pool(s) load completed at 2108
[New Thread 0x7fffd84d0640 (LWP 790752)]
[New Thread 0x7fffdc082640 (LWP 790753)]
2021-08-13 18:14:51 0 [Note] Reading of all Master_info entries succeeded
2021-08-13 18:14:51 0 [Note] Added new Master_info '' to hash table
2021-08-13 18:14:51 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 790762)]
[Thread 0x7fffd2419640 (LWP 790744) exited]
[Thread 0x7fffd6cf0640 (LWP 790735) exited]
[Thread 0x7fffd4c94640 (LWP 790739) exited]
```

[Thread 0x7ffffd64d9640 (LWP 790736) exited]
10.3.13-0268b871228-debug-asan

✓  Alice Sherepa added a comment - 2021-08-26 14:28

Thank you!

~ [MDEV-26437](#)

```
CREATE TABLE t1 (v2 varchar(50) AS ( NULL IN ( 'x' SOUNDS LIKE UTC_TIME())));  
SELECT DEFAULT (v2) FROM t1 ;  
INSERT IGNORE INTO t1 VALUES ( 1 ) ;
```

10.2 228630f61ac10240c36717


```
#3 <signal handler called>  
#4 0x000055e8eab39044 in Arg_comparator::compare_real_fixed (this=0x7f073  
#5 0x000055e8eab4d554 in Arg_comparator::compare (this=0x7f0738035f60) at  
#6 0x000055e8eab3b9a7 in Item_func_eq::val_int (this=0x7f0738035ea0) at /  
#7 0x000055e8eab1eaa8 in Item::save_in_field (this=0x7f0738035ea0, field=  
#8 0x000055e8ea98b6b9 in TABLE::update_virtual_fields (this=0x7f073817664  
#9 0x000055e8ea80c8e9 in fill_record (thd=0x7f0738000d90, table=0x7f07381  
#10 0x000055e8ea80ca10 in fill_record_n_invoke_before_triggers (thd=0x7f07  
#11 0x000055e8ea84ce29 in mysql_insert (thd=0x7f0738000d90, table_list=0x7  
#12 0x000055e8ea874638 in mysql_execute_command (thd=0x7f0738000d90) at /1  
#13 0x000055e8ea87fb42 in mysql_parse (thd=0x7f0738000d90, rawbuf=0x7f0738  
#14 0x000055e8ea86dd9d in dispatch_command (command=COM_QUERY, thd=0x7f073  
#15 0x000055e8ea86c898 in do_command (thd=0x7f0738000d90) at /10.2/src/sql  
#16 0x000055e8ea9c8661 in do_handle_one_connection (connect=0x55e8eda49d10  
#17 0x000055e8ea9c83c6 in handle_one_connection (arg=0x55e8eda49d10) at /1  
#18 0x000055e8eb1f1ec4 in pfs_spawn_thread (arg=0x55e8eda2cfd0) at /10.2/s  
#19 0x00007f07940b1609 in start_thread (arg=<optimized out>) at pthread cr
```

✓ People

Assignee:

 Nikita Malyavin

Reporter:

 yaoguang

Votes:

0 Vote for this issue

Watchers:

- 4 Start watching this issue

▼ Dates

Created:

2021-08-13 07:10

Updated:

2022-04-14 11:43

Resolved:

2021-10-01 19:19

▼ Git Integration



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