MariaDB Server MDEV-26407

Server crashes in Item_func_in::cleanup/Item::cleanup_processor

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Major
Resolution:	Duplicate
Affects Version/s:	10.2, 10.3, 10.4, 10.5, 10.6, 10.7
Fix Version/s:	10.3.35, 10.4.25, 10.5.16, (2)
Component/s:	Virtual Columns
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 ( v1 VARCHAR ( 65 ) CHAR SET ASCII NULL DEFAULT ( 'x' IN ( 'x' , CU
 START TRANSACTION READ WRITE ;
 INSERT INTO v0 VALUES ( v1 ) ;
 SELECT HEX ( GREATEST ( v1 , ( 'x' ) ) ) FROM v0 ;
 INSERT INTO v0 VALUES ( REPEAT ( ( NULL + 84551986.000000 ) = 74599462.000000 , (
 DESCRIBE SELECT v0 . v1 FROM v0 , v0 WHERE v0 . v1 = v0 . v1 ;
```

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
Version: '10.7.0-MariaDB'  socket: '/tmp/0.socket'  port: 3306  Source distribu
```

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 321844]
[New LWP 272301]
[New LWP 315980]
```

Issue Links

duplicates

MDEV-24176	Server crashes after insert in the table with virtual column ...	CLOSED
MDEV-26437	Server crashes in Item_args::walk_args	CLOSED

is duplicated by

MDEV-26408	use-after-poison security in sql/item_cmpfunc.h	CLOSED
MDEV-26414	use-after-poison in Data Mainipulation	CLOSED
MDEV-26417	use-after-poison issue of MariaDB server	CLOSED

Show 15 more links (8 is duplicated by, 6 relates to, 1 links to)

Activity

Alice Sherepa added a comment - 2021-08-26 12:15

Thank you for the report!
I think it is the same problem as ~~MDEV-26437~~, slightly different, so I will leave it here.
Repeatable on 10.2-10.6:

```
CREATE TABLE t1 ( v1 int DEFAULT ('x' IN ('x', CURRENT_USER))) ;
INSERT INTO t1 VALUES ( v1 ) ;
INSERT INTO t1 VALUES ( v1 ) ;
```

10.2 228630f61ac10240c36717

```
#3  <signal handler called>
#4  0x000056340c8dfbfd in Item_func_in::cleanup (this=0x7f59dc035188) at /
#5  0x000056340c78581f in Item::cleanup_processor (this=0x7f59dc035188, ar
#6  0x000056340c40f0b4 in Item::cleanup_excluding_fields_processor (this=0
#7  0x000056340c48632c in Item_func_or_sum::walk (this=0x7f59dc035188, pro
#8  0x000056340c5f5a90 in fix_session_vcol_expr (thd=0x7f59dc000d90, vcol=
#9  0x000056340c47af5c in TABLE::fix_vcol_exprs (this=0x7f59dc175dc0, thd=
#10 0x000056340c47b128 in fix_all_session_vcol_exprs (thd=0x7f59dc000d90,
#11 0x000056340c47b76e in lock_tables (thd=0x7f59dc000d90, tables=0x7f59dc
#12 0x000056340c47ab4d in open_and_lock_tables (thd=0x7f59dc000d90, option
#13 0x000056340c4405b9 in open_and_lock_tables (thd=0x7f59dc000d90, tables
#14 0x000056340c4c3272 in mysql_insert (thd=0x7f59dc000d90, table_list=0x7
#15 0x000056340c4eb638 in mysql_execute_command (thd=0x7f59dc000d90) at /1
#16 0x000056340c4f6b42 in mysql_parse (thd=0x7f59dc000d90, rawbuf=0x7f59dc
#17 0x000056340c4e4d9d in dispatch_command (command=COM_QUERY, thd=0x7f59d
#18 0x000056340c4e3898 in do_command (thd=0x7f59dc000d90) at /10.2/src/sql
#19 0x000056340c63f661 in do_handle_one_connection (connect=0x56340f11dd10
#20 0x000056340c63f3c6 in handle_one_connection (arg=0x56340f11dd10) at /1
```

Alice Sherepa added a comment - 2021-08-27 11:47

```
CREATE TABLE t1 (i INT DEFAULT (from_unixtime (last_day (CASE 1 WHEN 'x' THEN
UPDATE t1 SET i = 'x' WHERE i IS NULL ;
INSERT INTO t1 VALUES  ('a') ;
```

10.4 dc6be85ed29586631d

```
210827 13:46:07 [ERROR] mysqld got signal 11 ;

Server version: 10.4.22-MariaDB-debug-log

sql/signal_handler.cc:222(handle_fatal_signal)[0x559a62941fb3]
sigaction.c:0(__restore_rt)[0x7f11563fd3c0]
sql/item_cmpfunc.h:1973(Predicant_to_list_comparator::Predicant_to_value_c
sql/item_cmpfunc.h:2080(Predicant_to_list_comparator::cleanup())[0x559a62a
sql/item_cmpfunc.h:2258(Item_func_case_simple::cleanup())[0x559a62a572a9]
sql/item.cc:564(Item::cleanup_processor(void*))[0x559a6299538a]
sql/item.h:1904(Item::cleanup_excluding_fields_processor(void*))[0x559a61e
sql/item.h:5265(Item_func_or_sum::walk(bool (Item::*)(void*), bool, void*)
sql/item.h:2579(Item_args::walk_args(bool (Item::*)(void*), bool, void*))[
sql/item.h:5263(Item_func_or_sum::walk(bool (Item::*)(void*), bool, void*)
sql/item.h:2579(Item_args::walk_args(bool (Item::*)(void*), bool, void*))[
sql/item.h:5263(Item_func_or_sum::walk(bool (Item::*)(void*), bool, void*)
sql/table.cc:3289(fix_session_vcol_expr(THD*, Virtual_column_info*))[0x559
sql/sql_base.cc:5477(TABLE::fix_vcol_exprs(THD*))[0x559a61fb752f]
```

People

Assignee:

Sergei Golubchik

Reporter:

Zhiyong Wu

Votes:

1 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2021-08-19 02:21

Updated:

2022-07-02 07:47

Resolved:

2022-04-28 11:46

Git Integration

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