MariaDB Server MDEV-26281

ASAN use-after-poison when complex conversion is involved in blob

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Fixed
Affects Version/s:	10.6.0, 10.6.1, 10.6.2, 10.6.3, 10.2, 10.3, 10.4, 10.5, 10.6
Fix Version/s:	10.2.44, 10.3.35, 10.4.25, (3)
Component/s:	Virtual Columns
Labels:	crash virtual_columns
Environment:	Linux x64

Description

step to reproduce:

```
CREATE TEMPORARY TABLE v0 ( v2 TINYBLOB AS ( CURRENT_USER IS NULL IS UNKNOWN ) VIRT

ALTER TABLE v0 ADD COLUMN v0 MEDIUMINT ZEROFILL KEY UNIQUE COMMENT 'x' ;

INSERT IGNORE INTO v0 VALUES ( CONVERT ( 'x' LIKE v1 IS UNKNOWN , TIME ) , 'x' , v2

drop table v0;
```

asan report:

```
=================================================================3652686==ERR
READ of size 8 at 0x62b00007a760 thread T18
    #0 0x55b5f9bdde1d in Item_func_in::cleanup() /home/supersix/fuzz/security/M
    #1 0x55b5f8b42d30 in Item::delete_self() /home/supersix/fuzz/security/Maria
    #2 0x55b5f8b42d30 in Query_arena::free_items() /home/supersix/fuzz/security
    #3 0x55b5f908c814 in closefrm(TABLE*) /home/supersix/fuzz/security/MariaDB/
    #4 0x55b5f93e8b98 in THD::close_temporary_table(TABLE*) /home/supersix/fuzz
    #5 0x55b5f93ee75d in THD::drop_temporary_table(TABLE*, bool*, bool) /home/s
    #6 0x55b5f8f6f876 in mysql_rm_table_no_locks(THD*, TABLE_LIST*, st_mysql_co
```

```
#7 0x55b5f8f78e7b in mysql_rm_table(THD*, TABLE_LIST*, bool, bool, bool, bo
#8 0x55b5f8ccb268 in mysql_execute_command(THD*, bool) /home/supersix/fuzz/
#9 0x55b5f8c888dc in mysql_parse(THD*, char*, unsigned int, Parser_state*)
#10 0x55b5f8cbe2a3 in dispatch_command(enum_server_command, THD*, char*, un
#11 0x55b5f8cc3703 in do_command(THD*, bool) /home/supersix/fuzz/security/M
#12 0x55b5f918314c in do_handle_one_connection(CONNECT*, bool) /home/supers
#13 0x55b5f9184806 in handle_one_connection /home/supersix/fuzz/security/Ma
#14 0x55b5f9fcfeef in pfs_spawn_thread /home/supersix/fuzz/security/MariaDB
#15 0x7f20bfcea608 in start_thread /build/glibc-ZN95T4/glibc-2.31/nptl/pthr
```

Issue Links

duplicates

MDEV-24176	Server crashes after insert in the table with virtual column ...	CLOSED

is duplicated by

MDEV-26411	heap-use-after-free in sql/item_cmpfunc.h	CLOSED

relates to

MDEV-26006	Server crash or ASAN errors in in_vector::find upon SELECT ...	OPEN
MDEV-26407	Server crashes in Item_func_in::cleanup/Item::cleanup_proc...	CLOSED

links to

CVE-2022-27377

Activity

Alice Sherepa added a comment - 2021-07-30 15:02

Thanks you!
Repeatable on 10.2-10.6.

```
CREATE TABLE t1 (
  v2 blob AS ('a' is null),
  a1 int,
  a char(1) AS (cast(a1 in (0,current_user() is null) as char(16777216) ))
);

INSERT IGNORE INTO t1 VALUES ('x','x',v2) ;
```

```
drop table t1;
```

10.2 0e8981ef93ff4421e3

```
#3  <signal handler called>
#4  0x000056539c3588f7 in Item_func_in::cleanup (this=0x7fed000a9c98) at /
#5  0x000056539bf2645d in Item::delete_self (this=0x7fed000a9c98) at /10.2
#6  0x000056539bf1cf30 in Query_arena::free_items (this=0x7fed00034ee0) at
#7  0x000056539c070918 in closefrm (table=0x7fed001767b0) at /10.2/src/sql
#8  0x000056539c15bfb0 in intern_close_table (table=0x7fed001767b0) at /10
#9  0x000056539c15eacd in tdc_remove_table (thd=0x7fed00000d90, remove_typ
#10 0x000056539c02ad4c in mysql_rm_table_no_locks (thd=0x7fed00000d90, tab
#11 0x000056539c02a106 in mysql_rm_table (thd=0x7fed00000d90, tables=0x7fe
#12 0x000056539bf659b0 in mysql_execute_command (thd=0x7fed00000d90) at /1
#13 0x000056539bf6fa8c in mysql_parse (thd=0x7fed00000d90, rawbuf=0x7fed00
#14 0x000056539bf5dce7 in dispatch_command (command=COM_QUERY, thd=0x7fed0
#15 0x000056539bf5c7e2 in do_command (thd=0x7fed00000d90) at /10.2/src/sql
#16 0x000056539c0b83e9 in do_handle_one_connection (connect=0x56539e642c30
#17 0x000056539c0b814e in handle_one_connection (arg=0x56539e642c30) at /1
#18 0x000056539c8e225c in pfs_spawn_thread (arg=0x56539e626020) at /10.2/s
#19 0x00007fed5dbed609 in start_thread (arg=<optimized out>) at pthread_cr
#20 0x00007fed5d7c8293 in clone () at ../sysdeps/unix/sysv/linux/x86_64/cl
```

with temporary table – the same as reported:

10.2 0e8981ef93ff4421e3

```
#3  <signal handler called>
#4  0x00005614142438f7 in Item_func_in::cleanup (this=0x7f6594035b58) at /
#5  0x0000561413e1145d in Item::delete_self (this=0x7f6594035b58) at /10.2
#6  0x0000561413e07f30 in Query_arena::free_items (this=0x7f65941765f0) at
#7  0x0000561413f5b918 in closefrm (table=0x7f65941756b0) at /10.2/src/sql
#8  0x000056141404e0fa in THD::close_temporary_table (this=0x7f6594000d90,
#9  0x000056141404ec49 in THD::free_temporary_table (this=0x7f6594000d90,
#10 0x000056141404cd03 in THD::drop_temporary_table (this=0x7f6594000d90,
#11 0x0000561413f157ec in mysql_rm_table_no_locks (thd=0x7f6594000d90, tab
#12 0x0000561413f15106 in mysql_rm_table (thd=0x7f6594000d90, tables=0x7f6
#13 0x0000561413e509b0 in mysql_execute_command (thd=0x7f6594000d90) at /1
#14 0x0000561413e5aa8c in mysql_parse (thd=0x7f6594000d90, rawbuf=0x7f6594
#15 0x0000561413e48ce7 in dispatch_command (command=COM_QUERY, thd=0x7f659
#16 0x0000561413e477e2 in do_command (thd=0x7f6594000d90) at /10.2/src/sql
#17 0x0000561413fa33e9 in do_handle_one_connection (connect=0x561418029c30
#18 0x0000561413fa314e in handle_one_connection (arg=0x561418029c30) at /1
#19 0x00005614147cd25c in pfs_spawn_thread (arg=0x56141800d020) at /10.2/s
#20 0x00007f65f24f5609 in start_thread (arg=<optimized out>) at pthread_cr
```

when trying to select from this table :

select * from t1;

10.2 0e8981ef93ff4421e3

```
#4  0x000055828da2c763 in in_vector::find (this=0x7fa368013248, item=0x7fa
#5  0x000055828da2f28a in Item_func_in::val_int (this=0x7fa368035b58) at /
#6  0x000055828da5eadf in Item_int_func::val_str (this=0x7fa368035b58, str
#7  0x000055828dad8863 in Item_char_typecast::val_str (this=0x7fa368035ca8
#8  0x000055828da094cd in Item::save_in_field (this=0x7fa368035ca8, field=
#9  0x000055828d876441 in TABLE::update_virtual_fields (this=0x7fa3681756b
#10 0x000055828d9e92f0 in handler::ha_rnd_next (this=0x7fa368176718, buf=0
#11 0x000055828d9eaa52 in handler::read_first_row (this=0x7fa368176718, bu
#12 0x000055828d7e907b in handler::ha_read_first_row (this=0x7fa368176718,
#13 0x000055828d7d0056 in join_read_system (tab=0x7fa368013b10) at /10.2/s
#14 0x000055828d7cfc0d in join_read_const_table (thd=0x7fa368000d90, tab=0
#15 0x000055828d7a96cf in make_join_statistics (join=0x7fa368012fe8, table
#16 0x000055828d7a0a39 in JOIN::optimize_inner (this=0x7fa368012fe8) at /1
#17 0x000055828d79ef30 in JOIN::optimize (this=0x7fa368012fe8) at /10.2/sr
#18 0x000055828d7a8486 in mysql_select (thd=0x7fa368000d90, tables=0x7fa36
#19 0x000055828d79c66a in handle_select (thd=0x7fa368000d90, lex=0x7fa3680
#20 0x000055828d766cd0 in execute_sqlcom_select (thd=0x7fa368000d90, all_t
#21 0x000055828d75d844 in mysql_execute_command (thd=0x7fa368000d90) at /1
```

Please check the initial case before closing the bug.

Alice Sherepa added a comment - 2021-07-30 15:18

derived from the test case:

```
CREATE TABLE `t1` (
  `v2` tinyblob GENERATED ALWAYS AS (current_user() is null is null) VIRTUAL,
  `v1` tinyint(3) unsigned zerofill DEFAULT NULL,
  `MEDIUM` char(1) CHARACTER SET utf8 COLLATE utf8_bin GENERATED ALWAYS AS (ca
  `t1` mediumint(8) unsigned zerofill NOT NULL COMMENT 'x',
  PRIMARY KEY (`t1`)
) ;

INSERT IGNORE INTO t1 VALUES
( CONVERT ( 'x' LIKE v1 IS UNKNOWN , TIME ) , 'x' ,
  v2 IN ( v2 SOUNDS LIKE v1 IS FALSE ) IS UNKNOWN ,
  1 ) ;

select * from t1;
```

fails the same way on 10.2 (in_vector::find ,..),
on 10.3:

10.3 43099af95bc554ff870b00b

```
210730 17:07:32 [ERROR] mysqld got signal 11 ;

Server version: 10.3.31-MariaDB-debug-log

strings/decimal.c:1917(do_sub)[0x561d6e08e480]
strings/decimal.c:2046(decimal_cmp)[0x561d6e08f64f]
sql/my_decimal.h:500(my_decimal_cmp(my_decimal const*, my_decimal const*))
sql/item_cmpfunc.cc:3524(cmp_decimal(void*, my_decimal*, my_decimal*))[0x5
sql/item_cmpfunc.cc:3539(in_vector::find(Item*))[0x561d6ccf19af]
sql/item_cmpfunc.cc:4442(Item_func_in::val_int())[0x561d6ccf97ea]
sql/item_func.cc:751(Item_int_func::val_str(String*))[0x561d6cd5cd84]
sql/item_timefunc.cc:2503(Item_char_typecast::val_str(String*))[0x561d6ceb
sql/item_strfunc.h:72(Item_str_func::update_null_value())[0x561d6c46875b]
sql/item_func.h:185(Item_func::is_null())[0x561d6c3be80d]
sql/item_cmpfunc.cc:5215(Item_func_isnotnull::val_int())[0x561d6cd00d68]
sql/item.cc:6890(Item::save_int_in_field(Field*, bool))[0x561d6cc92d59]
sql/sql_type.cc:2593(Type_handler_int_result::Item_save_in_field(Item*, Fi
sql/item.cc:6900(Item::save_in_field(Field*, bool))[0x561d6cc92f3d]
```

on 10.6

0.6 beb401b25fa3e34ea431da

```
mariadbd: /10.6/src/strings/decimal.c:1082: ull2dec: Assertion `(to)->len
210730 17:15:50 [ERROR] mysqld got signal 6 ;

Server version: 10.6.4-MariaDB-debug-log

sql/signal_handler.cc:225(handle_fatal_signal)[0x5604516a0961]
sigaction.c:0(__restore_rt)[0x7f5a907c83c0]
linux/raise.c:51(__GI_raise)[0x7f5a902b518b]
stdlib/abort.c:81(__GI_abort)[0x7f5a90294859]
intl/loadmsgcat.c:509(get_sysdep_segment_value)[0x7f5a90294729]
:0(__GI___assert_fail)[0x7f5a902a5f36]
strings/decimal.c:1084(ull2dec)[0x560452cd4477]
strings/decimal.c:1112(ulonglong2decimal)[0x560452cd486f]
sql/my_decimal.h:452(int2my_decimal(unsigned int, long long, char, my_deci
sql/field.cc:2222(Field_int::val_decimal(my_decimal*))[0x560451615389]
sql/item.cc:3303(Item_field::val_decimal(my_decimal*))[0x560451714df4]
sql/item_cmpfunc.cc:3910(in_decimal::get_value(Item*))[0x560451792b49]
```

Nikita Malyavin added a comment - 2022-04-13 20:07

The fixes have been made and pushed.

Note for mergers

Please, zero-merge these changes, while merging 10.2->10.3->10.4.

The fix.

The code base differs a lot in this place, zone, so separate versions are made for 10.2-10.4

10.2: https://github.com/MariaDB/server/commit/c8cf6c31ced1b5a6698b124a2c4aaaec6d3f85b9
10.3: https://github.com/MariaDB/server/commit/85833341a0556a1e0c789ca7b6ab05e6e7519ae7
10.4: https://github.com/MariaDB/server/commit/b19f675b030f9ce3a94232d35d8e3c74bdfcbdbe

Sergei Golubchik, you can focus on 10.4 version, since it includes most of the changes accumulated from previous versions. Up to you, though.

People

Assignee:

Sergei Golubchik

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

Dates

Created:

2021-07-30 10:18

Updated:

2022-04-15 14:41

Resolved:

2022-04-15 07:51

Git Integration

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