MariaDB Server MDEV-26061

MariaDB server crash at Field::set_default

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Fixed
Affects Version/s:	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
Environment:	Linux 5.4.0-39-generic #43-Ubuntu SMP Fri Jun 19 10:28:31 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

Description

Steps to reproduce:

```
CREATE TEMPORARY TABLE v0 ( v2 TIMESTAMP CHECK ( DEFAULT ( v2 ) IS NOT TRUE ) , v1
```

Reported by:

Yaoguang Chen of Ant Security Light-Year Lab

Backtrace:

Core was generated by `/home/supersix/fuzz/security/MariaDB/install/bin/mysqld --defaults-file=/home/s'.

Program terminated with signal SIGSEGV, Segmentation fault.

```
#0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0xb)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
[Current thread is 1 (Thread 0x7f154c17f300 (LWP 1992265))]
gdb-peda$ #0  __pthread_kill (threadid=<optimized out>, signo=signo@entry=0xb)
    at ../sysdeps/unix/sysv/linux/pthread_kill.c:56
#1  0x00005640d742e98f in my_write_core (sig=sig@entry=0xb)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/mysys/stacktrace.c:4
#2  0x00005640d5e9b583 in handle_fatal_signal (sig=<optimized out>)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/signal_handler.c
#3  <signal handler called>
```

```
#4  0x00005640d5dfe617 in Field::set_default (this=0x61d0000b9ab8)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/field.cc:2591
#5  0x00005640d5f553a6 in Item_default_value::calculate (this=0x6190000f5240)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/item.cc:9468
#6  0x00005640d5f55466 in Item_default_value::val_real (this=0x6190000f5240)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/item.cc:9486
#7  0x00005640d5bbf3bb in Type_handler_real_result::Item_val_bool (
    this=<optimized out>, item=<optimized out>)
    at /home/supersix/fuzz/security/MariaDB/mariadb-10.6.2/sql/sql_type.cc:5080
```

Issue Links

is duplicated by

MDEV-26424 MariaDB server crash in Field::set_default		CLOSED
MDEV-26429 MariaDB Server SEGV issue		CLOSED
MDEV-26430 MariaDB Server SEGV issue		CLOSED
MDEV-26435 MariaDB Server SEGV issue		CLOSED
MDEV-26436 MariaDB Server SEGV issue		CLOSED

Show 4 more links (3 relates to, 1 links to)

Activity

Alice Sherepa added a comment - 2021-07-01 08:04

Thank you!
Repeatable on 10.3-10.6:

```
CREATE TABLE t1 (d timestamp CHECK (DEFAULT (d) is true)) AS SELECT 1;
```

10.3 29098083f7ac3b445ee59c3e765eb6

```
Version: '10.3.31-MariaDB-debug-log'
210701 10:01:18 [ERROR] mysqld got signal 11 ;

sigaction.c:0(__restore_rt)[0x7f19466823c0]


sql/field.cc:2420(Field::set_default())[0x55d4807c0aba]
sql/item.cc:9429(Item_default_value::calculate())[0x55d4808ff2dc]
sql/item.cc:9441(Item_default_value::val_real())[0x55d4808ff402]
sql/sql_type.cc:3302(Type_handler_temporal_result::Item_val_bool(Item*) co
```

10.3 2909808367ac3b445ee59c3e765eb6

```
sql/item.h:1220(Item::val_bool())[0x55d47fe65c74]
sql/item_cmpfunc.cc:1151(Item_func_truth::val_bool())[0x55d48092bfaf]
sql/item_cmpfunc.cc:1174(Item_func_truth::val_int())[0x55d48092c1d4]
sql/table.cc:5409(TABLE::verify_constraints(bool))[0x55d4803f54fe]
sql/table.cc:5384(TABLE_LIST::view_check_option(THD*, bool))[0x55d4803f50b
sql/sql_insert.cc:3931(select_insert::send_data(List<Item>&))[0x55d4800682
sql/sql_select.cc:4012(JOIN::exec_inner())[0x55d4801bb916]
sql/sql_select.cc:3933(JOIN::exec())[0x55d4801ba6a4]
```

Alice Sherepa added a comment - 2021-08-24 16:59

test case from ~~MDEV-26436~~, which repeats the problem starting from 10.2:

```
CREATE TABLE t1 (v2 DATE CHECK (v1 like DEFAULT (v1)), v1 DATE DEFAULT (FROM_D
INSERT IGNORE INTO t1 VALUES ( 'x' , 'x' ) ;
```

10.2 1f1d5606e08c928e3da98b

```
210824 18:56:05 [ERROR] mysqld got signal 11 ;
Server version: 10.2.41-MariaDB-debug-log

sigaction.c:0(__restore_rt)[0x7f69a711a3c0]
sql/field.cc:2457(Field::set_default())[0x5574ce5bcb1d]
sql/item.cc:9041(Item_default_value::calculate())[0x5574ce61b9a1]
sql/item.cc:9047(Item_default_value::val_str(String*))[0x5574ce61ba02]
sql/item_cmpfunc.cc:5276(Item_func_like::val_int())[0x5574ce63bf9e]
sql/table.cc:5303(TABLE::verify_constraints(bool))[0x5574ce47a624]
sql/table.cc:5280(TABLE_LIST::view_check_option(THD*, bool))[0x5574ce47a51
sql/sql_insert.cc:1042(mysql_insert(THD*, TABLE_LIST*, List<Item>&, List<L
sql/sql_parse.cc:4217(mysql_execute_command(THD*))[0x5574ce369638]
sql/sql_parse.cc:7793(mysql_parse(THD*, char*, unsigned int, Parser_state*
sql/sql_parse.cc:1830(dispatch_command(enum_server_command, THD*, char*, u
sql/sql_parse.cc:1381(do_command(THD*))[0x5574ce361898]
sql/sql_connect.cc:1336(do_handle_one_connection(CONNECT*))[0x5574ce4bd661
sql/sql_connect.cc:1242(handle_one_connection)[0x5574ce4bd3c6]
perfschema/pfs.cc:1871(pfs_spawn_thread)[0x5574cece6ec4]
```

and also all similar cases, e.g

```
CREATE TABLE t1 (v2 DATE CHECK (v1 = DEFAULT (v1)), v1 DATE DEFAULT (FROM_DAYS
INSERT IGNORE INTO t1 VALUES ( 'x' , 'x' ) ;
```

10.2 1f1d5606e08c928e3da98b

```
210824 18:57:05 [ERROR] mysqld got signal 11 ;

Server version: 10.2.41-MariaDB-debug-log

sigaction.c:0(__restore_rt)[0x7fd7e0c813c0]
sql/field.cc:2457(Field::set_default())[0x55bae1298b1d]
sql/item.cc:9041(Item_default_value::calculate())[0x55bae12f79a1]
sql/item.cc:9071(Item_default_value::get_date(st_mysql_time*, unsigned lon
sql/item.cc:151(Item::get_date_with_conversion(st_mysql_time*, unsigned lo


sql/item.h:1511(Item::val_datetime_packed())[0x55bae0f68aef]
sql/item.h:1532(Item::val_temporal_packed(enum_field_types))[0x55bae12ff39
sql/item_cmpfunc.cc:797(Arg_comparator::compare_temporal(enum_field_types)
sql/item_cmpfunc.h:105(Arg_comparator::compare_datetime())[0x55bae0f57aff]
sql/item_cmpfunc.h:87(Arg_comparator::compare())[0x55bae131e554]
sql/item_cmpfunc.cc:1806(Item_func_eq::val_int())[0x55bae130c9a7]
sql/table.cc:5303(TABLE::verify_constraints(bool))[0x55bae1156624]
```

Alice Sherepa added a comment - 2021-08-25 09:12 - edited

test case from ~~MDEV-26435~~, with ALTER

```
CREATE TABLE t1 ( v1 TIMESTAMP ) ;
ALTER TABLE t1 ADD COLUMN t1 TEXT DEFAULT ( DEFAULT ( v1 ) ) ;
```

10.2 1f1d5606e08c928e3da98b

```
#3  <signal handler called>
#4  Field::set_default (this=0x7fb774038f58) at /10.2/src/sql/field.cc:2457
#5  0x0000564d85bd09a1 in Item_default_value::calculate (this=0x7fb774038e48) 
#6  0x0000564d85bd0b53 in Item_default_value::save_in_field (this=0x7fb774038e
#7  0x0000564d85a35bc0 in TABLE::update_default_fields (this=0x7fb774036ea0, i
#8  0x0000564d859f8bb7 in mysql_alter_table (thd=0x7fb774000d90, new_db=0x7fb7
#9  0x0000564d85a77c6c in Sql_cmd_alter_table::execute (this=0x7fb774013180, t
#10 0x0000564d85924cdc in mysql_execute_command (thd=0x7fb774000d90) at /10.2/
#11 0x0000564d85929b42 in mysql_parse (thd=0x7fb774000d90, rawbuf=0x7fb7740127


#12 0x0000564d85917d9d in dispatch_command (command=COM_QUERY, thd=0x7fb774000
#13 0x0000564d85916898 in do_command (thd=0x7fb774000d90) at /10.2/src/sql/sql
#14 0x0000564d85a72661 in do_handle_one_connection (connect=0x564d896e1d30) at
#15 0x0000564d85a723c6 in handle_one_connection (arg=0x564d896e1d30) at /10.2/
```

10.2 1f1d5606e08c928e3da98b

```
#16 0x0000564d86290ee4 in pfs_spawn_thread (arg=0x564d896c4ff0) at /10.2/src/s
#17 0x00007fb7c8214609 in start_thread (arg=<optimized out>) at pthread_create
#18 0x00007fb7c7def293 in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone
```

from ~~MDEV-26430~~

```
CREATE TABLE t1 (v1 TIMESTAMP, a INT NULL CHECK (ceil(DEFAULT (v1)) = NULL)) ;
INSERT t1 VALUES (NULL ,0) ;
```

10.2 1f1d5606e08c928e3da98b

```
#3  <signal handler called>
#4  Field::set_default (this=0x7f833c035440) at /10.2/src/sql/field.cc:245
#5  0x0000558dc2f009a1 in Item_default_value::calculate (this=0x7f833c0351
#6  0x0000558dc2f00a34 in Item_default_value::val_real (this=0x7f833c03515
#7  0x0000558dc2f548bc in Item_func_ceiling::real_op (this=0x7f833c0352b8)
#8  0x0000558dc2f5484a in Item_func_ceiling::int_op (this=0x7f833c0352b8)
#9  0x0000558dc2f4ea08 in Item_func_hybrid_field_type::val_real (this=0x7f
#10 0x0000558dc2f1304c in Arg_comparator::compare_real_fixed (this=0x7f833
#11 0x0000558dc2f27554 in Arg_comparator::compare (this=0x7f833c035678) at
#12 0x0000558dc2f159a7 in Item_func_eq::val_int (this=0x7f833c0355b8) at /
#13 0x0000558dc2d5f624 in TABLE::verify_constraints (this=0x7f833c175dc0,
#14 0x0000558dc2d5f517 in TABLE_LIST::view_check_option (this=0x7f833c0127
#15 0x0000558dc2c26f9e in mysql_insert (thd=0x7f833c000d90, table_list=0x7
#16 0x0000558dc2c4e638 in mysql_execute_command (thd=0x7f833c000d90) at /1
#17 0x0000558dc2c59b42 in mysql_parse (thd=0x7f833c000d90, rawbuf=0x7f833c
#18 0x0000558dc2c47d9d in dispatch_command (command=COM_QUERY, thd=0x7f833
```

```
CREATE TABLE t1 ( v1 TIMESTAMP, a INT CHECK (DEFAULT (v1) = NULL) ) ;
INSERT t1 VALUES ( NULL , 0 ) ;
```

10.2 1f1d5606e08c928e3da98b

```
#3  <signal handler called>
#4  Field::set_default (this=0x7efccc0355b8) at /10.2/src/sql/field.cc:245
#5  0x000055ef96d479a1 in Item_default_value::calculate (this=0x7efccc0351
#6  0x000055ef96d47ac6 in Item_default_value::get_date (this=0x7efccc03515
#7  0x000055ef96d2dfc6 in Item::get_date_with_conversion (this=0x7efccc035
#8  0x000055ef969b8aef in Item::val_datetime_packed (this=0x7efccc035158)
#9  0x000055ef96d4f39d in Item::val_temporal_packed (this=0x7efccc035158,
#10 0x000055ef96d59714 in Arg_comparator::compare_temporal (this=0x7efccc0
```

```
#11 0x000055ef96ba7aff in Arg_comparator::compare_datetime (this=0x7efccc0
10.2 1f1d5606e08c928e3da98b
#12 0x000055ef96d6e554 in Arg_comparator::compare (this=0x7efccc0353b0) at
#13 0x000055ef96d5c9a7 in Item_func_eq::val_int (this=0x7efccc0352f0) at /
#14 0x000055ef96ba6624 in TABLE::verify_constraints (this=0x7efccc175dc0,
#15 0x000055ef96ba6517 in TABLE_LIST::view_check_option (this=0x7efccc0127
#16 0x000055ef96a6df9e in mysql_insert (thd=0x7efccc000d90, table_list=0x7
#17 0x000055ef96a95638 in mysql_execute_command (thd=0x7efccc000d90) at /1
#18 0x000055ef96aa0b42 in mysql_parse (thd=0x7efccc000d90, rawbuf=0x7efccc
#19 0x000055ef96a8ed9d in dispatch_command (command=COM_QUERY, thd=0x7efcc
#20 0x000055ef96a8d898 in do_command (thd=0x7efccc000d90) at /10.2/src/sql
```

People

Assignee:

Sergei Golubchik

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

4 Start watching this issue

Dates

Created:

2021-07-01 02:40

Updated:

2022-04-14 13:45

Resolved:

2022-04-14 13:45

Git Integration

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