MariaDB Server MDEV-26419

A SEGV in Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort

Details

Type:	Bug
Status:	CLOSED (View Workflow)
Priority:	Blocker
Resolution:	Duplicate
Affects Version/s:	10.2, 10.3, 10.4, 10.5, 10.6, 10.7
Fix Version/s:	10.2.44, 10.3.35, 10.4.25, (3)
Component/s:	Optimizer - Window functions
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 ( v1 TINYINT NULL ) ;
 TRUNCATE TABLE v0 ;
 SELECT instr ( COALESCE ( sqrt ( ( quote ( 'x' / 46 ) ) + 0 ) , 'x' ) , 51 ) ;
 SAVEPOINT v0 ;
 SELECT 16 / 'x' AS v2 UNION SELECT -2147483648 AS v3 ORDER BY ( LAST_VALUE ( 'x' ) OVER (
 REPLACE INTO v0 VALUES ( TRUE ) ;
```

Log and Coredump:

```
2021-08-16 14:41:38 0 [Note] InnoDB: Compressed tables use zlib 1.2.11
2021-08-16 14:41:38 0 [Note] InnoDB: Number of pools: 1
2021-08-16 14:41:38 0 [Note] InnoDB: Using crc32 + pclmulqdq instructions
2021-08-16 14:41:38 0 [Note] mysqld: O_TMPFILE is not supported on /tmp (disabling fu
2021-08-16 14:41:38 0 [Note] InnoDB: Using liburing
2021-08-16 14:41:38 0 [Note] InnoDB: Initializing buffer pool, total size = 134217728
2021-08-16 14:41:38 0 [Note] InnoDB: Completed initialization of buffer pool
2021-08-16 14:41:38 0 [Note] InnoDB: 128 rollback segments are active.
2021-08-16 14:41:38 0 [Note] InnoDB: Creating shared tablespace for temporary tables
2021-08-16 14:41:38 0 [Note] InnoDB: Setting file './ibtmp1' size to 12 MB. Physicall
2021-08-16 14:41:38 0 [Note] InnoDB: File './ibtmp1' size is now 12 MB.
2021-08-16 14:41:38 0 [Note] InnoDB: 10.7.0 started; log sequence number 42161; trans
2021-08-16 14:41:38 0 [Note] InnoDB: Loading buffer pool(s) from /home/fuboat/mariadb
2021-08-16 14:41:38 0 [Note] Plugin 'FEEDBACK' is disabled.
```

```
2021-08-16 14:41:38 0 [Note] InnoDB: Buffer pool(s) load completed at 210816 14:41:38
2021-08-16 14:41:38 0 [Note] Server socket created on IP: '0.0.0.0'.
2021-08-16 14:41:38 0 [Note] Server socket created on IP: '::'.
2021-08-16 14:41:38 0 [Note] /usr/local/mysql/bin//mysqld: ready for connections.
```

Core pattern: core

GNU gdb (GDB) 10.2

```
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/local/mysql/bin//mysqld...
[New LWP 639727]
[New LWP 586228]
[New LWP 629512]
[New LWP 630498]
```

Issue Links

duplicates

MDEV-15208 server crashed, when using ORDER BY with window function and U... CLOSED

links to

CVE-2022-32088

Activity

Alice Sherepa added a comment - 2021-08-25 14:02 - edited

THank you!
I repeated on 10.2-10.6:

```
SELECT 1 UNION SELECT 1 ORDER BY max(1) OVER ();
```

10.2 1f1d5606e08c928e3da98b

```
#2  0x000055976aa82831 in handle_fatal_signal (sig=11) at /10.2/src/sql/signal_h
#3  <signal handler called>
#4  0x000055976a99345c in Exec_time_tracker::get_loops (this=0xa5a5a5a5a5a5a5a5)
#5  0x000055976aa819e4 in Filesort_tracker::report_use (this=0xa5a5a5a5a5a5a5a5,
#6  0x000055976aa7bf3c in filesort (thd=0x7f637c000d90, table=0x7f637c034a98, fi
#7  0x000055976a876cfd in create_sort_index (thd=0x7f637c000d90, join=0x7f637c01
#8  0x000055976a9d33ac in Window_funcs_sort::exec (this=0x7f637c016de0, join=0x7
#9  0x000055976a9d38ec in Window_funcs_computation::exec (this=0x7f637c016dc0, j
#10 0x000055976a883ff2 in AGGR_OP::end_send (this=0x7f637c016c60) at /10.2/src/s
#11 0x000055976a86e97b in sub_select_postjoin_aggr (join=0x7f637c014970, join_ta
#12 0x000055976a86ecaf in sub_select (join=0x7f637c014970, join_tab=0x7f637c015c
#13 0x000055976a86e493 in do_select (join=0x7f637c014970, procedure=0x0) at /10.
#14 0x000055976a847f4b in JOIN::exec_inner (this=0x7f637c014970) at /10.2/src/sq
#15 0x000055976a8473f2 in JOIN::exec (this=0x7f637c014970) at /10.2/src/sql/sql_
#16 0x000055976a8485cc in mysql_select (thd=0x7f637c000d90, tables=0x7f637c0049d
#17 0x000055976a8ef39d in st_select_lex_unit::exec (this=0x7f637c004988) at /10.
#18 0x000055976a8eb21c in mysql_union (thd=0x7f637c000d90, lex=0x7f637c0048c8, r
#19 0x000055976a83c63c in handle_select (thd=0x7f637c000d90, lex=0x7f637c0048c8,
```

Steve Beattie added a comment - 2022-07-01 23:55

Hi, it appears this issue was assigned CVE-2022-32088.

(I'm just a messenger, I'm not the one who requested or allocated the CVE identifier.)

Mingli-Yu added a comment - 2022-07-07 07:47

Does the version 10.8.3 have the issue? Thanks!

Alice Sherepa added a comment - 2022-07-07 09:02

No, 10.8.3 returns an error, as expected. The bug was fixed at 942a9791b2231273ba20649a658c commit (https://github.com/MariaDB/server/commit/942a9791b2231273ba20649a658c856641268fae)

People

Assignee:

Oleg Smirnov

Reporter:

Zhiyong Wu

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

Dates

Created:

2021-08-19 03:07

Updated:

2022-08-05 07:43

Resolved:

2022-07-07 09:03

Git Integration

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