MariaDB Server MDEV-26323

use-after-poison issue of MariaDB server

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, (4)
Component/s:	Plugins
Labels:	crash
Environment:	Linux x64

Description

step to reproduce:

```
INSTALL PLUGIN DEALLOCATE SONAME 'x' ;
```

asan report:

```
Version: '10.6.5-MariaDB'  socket: '/tmp/mysql_mar.sock'  port: 3309  Source di
=================================================================
==283607==ERROR: AddressSanitizer: use-after-poison on address 0x62b000077306 a
READ of size 1 at 0x62b000077306 thread T48
    #0 0x56165517504d in my_strcasecmp_8bit /home/supersix/fuzz/security/MariaD
    #1 0x561653282063 in fix_dl_name /home/supersix/fuzz/security/MariaDB/serve
    #2 0x561653282063 in plugin_add /home/supersix/fuzz/security/MariaDB/server
    #3 0x561653293f30 in mysql_install_plugin(THD*, st_mysql_const_lex_string c
    #4 0x56165326a1df in mysql_execute_command(THD*, bool) /home/supersix/fuzz/
    #5 0x561653225684 in mysql_parse(THD*, char*, unsigned int, Parser_state*)
    #6 0x56165325b0b3 in dispatch_command(enum_server_command, THD*, char*, uns
    #7 0x561653260513 in do_command(THD*, bool) /home/supersix/fuzz/security/Ma
    #8 0x5616537226fc in do_handle_one_connection(CONNECT*, bool) /home/supersi

    #9 0x561653723e56 in handle_one_connection /home/supersix/fuzz/security/Mar
    #10 0x56165456fd2f in pfs_spawn_thread /home/supersix/fuzz/security/MariaDB
    #11 0x7f3e5895a608 in start_thread /build/glibc-ZN95T4/glibc-2.31/nptl/pthr
    #12 0x7f3e5852e292 in __clone (/lib/x86_64-linux-gnu/libc.so.6+0x122292)
```

Issue Links

links to

CVE-2022-27383

Activity

Oleksandr Byelkin added a comment - 2022-04-14 08:03

It looks like a charset problem (length of the string play the key role, in case of 4 symbol there is no problem)

People

Assignee:

Alexander Barkov

Reporter:

yaoguang

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2021-08-09 09:28

Updated:

2022-04-14 13:31

Resolved:

2022-04-14 13:31

Git Integration

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