MariaDB Connector/C / CONC-819

mysql_real_escape_string incorrectly handles big5

Details

Type:	Bug	Status:	CLOSED (View Workflow)
Priority:	Critical	Resolution:	Fixed
Affects Version/s:	3.3, 3.4	Fix Version/s:	3.3.19, 3.4.9
Component/s:	Character Sets		
Labels:	None		

Description

test case for `unittest/libmariadb/charset.c`

```
#define TEST_BUG8378a_IN  "\xa1' + 10 -- "
#define TEST_BUG8378a_OUT "\\\xa1\\' + 10 -- "

/* set connection options */
struct my_option_st opt_bug8378a[] = {
  {MYSQL_SET_CHARSET_NAME, (char *) "big5"},
  {0, NULL}
};

int bug_8378a(MYSQL *mysql) {
  int rc, len;
  char out[128], buf[256];
  MYSQL_RES *res;
  MYSQL_ROW row;

  /* MXS-4898: MaxScale sends utf8mb4 in handshake OK packet */
  SKIP_MAXSCALE;

  len= mysql_real_escape_string(mysql, out, TEST_BUG8378a_IN, sizeof(TEST_BUG8378a_IN)-1);
  FAIL_IF(memcmp(out, TEST_BUG8378a_OUT, len), "wrong result");
```

Reported by Jun Rong

Issue Links

links to

CVE-2026-44172

Activity

There are no comments yet on this issue.

People

Assignee:

Georg Richter

Reporter:

Sergei Golubchik

Votes:

0 Vote for this issue

Watchers:

1 Start watching this issue

Dates

Created:

2026-04-21 17:32

Updated:

2026-06-01 08:42

Resolved:

2026-04-22 10:19

Git Integration

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