MariaDB Server / MDEV-39413

wsrep unsafe handling of parameters

Details

Type:	Bug	Status:	CLOSED (View Workflow)
Priority:	Critical	Resolution:	Fixed
Affects Version/s:	10.6, 10.11, 11.4, 11.8, 12.3	Fix Version/s:	10.6.26, 10.11.17, ... (3)
Component/s:	wsrep		
Labels:	None		
Bug Category:	Can result in unexpected behaviour		
Sprint:	Q2/2026 Replic. Development		

Description

`wsrep_sst_mariabackup` on the donor side interpolates parameters sent by the joiner into the command line without proper validation.

For example, certificate's CommonName can contain arbitrary characters.

Reported by Asim Viladi Oglu Manizada

Issue Links

relates to

MDEV-39612	Galera Cluster-peer > Donor command execution	CLOSED
MDEV-39676	Galera Cluster-peer > Donor command execution	CLOSED
MDEV-39721	wsrep_notify_cmd should sanitize peer-supplied fields before shell substitution	CLOSED

links to

CVE-2026-44168

Activity

Sergei Golubchik added a comment - 2026-04-23 14:00

I gave up. This is how I tried to make the test:

```
--- a/mysql-test/suite/galera/t/galera_sst_mariabackup_encrypt_with_key_server.test
+++ b/mysql-test/suite/galera/t/galera_sst_mariabackup_encrypt_with_key_server.test
@@ -16,9 +16,32 @@ SELECT 1;
 --source include/wait_condition.inc

 # Confirm that transfer was SSL-encrypted
---let $assert_text = Using openssl based encryption with socat
---let $assert_select = Using openssl based encryption with socat: with key and crt
---let $assert_count = 1
---let $assert_file = $MYSQLTEST_VARDIR/log/mysqld.1.err
---let $assert_only_after = CURRENT_TEST
---source include/assert_grep.inc
+--let SEARCH_FILE = $MYSQLTEST_VARDIR/log/mysqld.1.err
+--let SEARCH_PATTERN = Using openssl based encryption with socat: with key and crt
+--source include/search_pattern_in_file.inc
+
+--echo #
+--echo # MDEV-39413 wsrep unsafe handling of parameters
+--echo #
+
```

but node_2 doesn't start no matter what I tried.
Also aborted SST leaves `mbstream` and `socat` processes running, but they timeout eventually.

People

Assignee:

Sergei Golubchik

Reporter:

Sergei Golubchik

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

2026-04-22 19:52

Updated:

2 days ago 10:05

Resolved:

2026-04-27 07:44

Git Integration

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