**SUMMARY**

A concurrency bug in MySQL-5.1+

**DETAILS**

Some details can also be found at: <https://bugs.mysql.com/bug.php?id=59464>

This bug is due to a data race.

The function row\_vers\_build\_for\_semi\_consistent\_read(), introduced in the fix of Bug #3300, is checking version\_trx->conc\_state while not holding kernel\_mutex.

Version\_trx could be null.

|  |  |
| --- | --- |
| Thread1 (row0vers.c) | Thread2 (StatementImple.java) |
| ulint  row\_vers\_build\_for\_semi\_consistent\_read(..)  {  ..  mutex\_enter(&kernel\_mutex);  version\_trx = trx\_get\_on\_id(version\_trx\_id);  mutex\_exit(&kernel\_mutex);  if (!version\_trx || version\_trx->conc\_state == TRX\_NOT\_STARTED || version\_trx->conc\_state == TRX\_COMMITTED\_IN\_MEMORY) {  ..  }  } | ulint  row\_vers\_build\_for\_semi\_consistent\_read(..)  {  ..  mutex\_enter(&kernel\_mutex);  version\_trx = trx\_get\_on\_id(version\_trx\_id);  mutex\_exit(&kernel\_mutex);  if (!version\_trx || version\_trx->conc\_state == TRX\_NOT\_STARTED || version\_trx->conc\_state == TRX\_COMMITTED\_IN\_MEMORY) {  ..  }  } |
| 0-lock | 1-lock |