**SUMMARY**

A concurrency bug in MySQL-5.0, 5.1

**DETAILS**

Some details can also be found at: <https://bugs.mysql.com/bug.php?id=24721>

This bug is due to a data race.

Double checked locking: when one thread has the mutex and is initializing structure, the assignment to charset\_initialized that it does may be visible to other threads before all of the other writes that it does. This will allow other threads to read invalid data.

|  |  |
| --- | --- |
| Thread1 (charset.c) | Thread2 (StatementImple.java) |
| static my\_bool init\_available\_charsets(myf myflags)  #endif  {  ..  \*/  if (!charset\_initialized)  {  ..  pthread\_mutex\_lock(&THR\_LOCK\_charset);  if (!charset\_initialized)  {  ..  charset\_initialized=1;  }  pthread\_mutex\_unlock(&THR\_LOCK\_charset);  }  return error;  } | static my\_bool init\_available\_charsets(myf myflags)  #endif  {  ..  \*/  if (!charset\_initialized)  {  ..  pthread\_mutex\_lock(&THR\_LOCK\_charset);  if (!charset\_initialized)  {  ..  charset\_initialized=1;  }  pthread\_mutex\_unlock(&THR\_LOCK\_charset);  }  return error;  } |
| 0-lock | 1-lock |