

## MySQL 3.23.55 Released - Security

NEWS\_PDF\_AUTHOR: w4z004

NEWS\_PDF\_DATE: 2003/2/1 2:44:10

MySQL 3.23.55, a new version of the popular Open Source Database, has been released. It is now available in source and binary form for a number of platforms from our download pages at <http://www.mysql.com/downloads/> and mirror sites.

Note that not all mirror sites may be up to date at this point of time - if you can't find this version on some mirror, please try again later or choose another download site.

This is a bugfix release for the current stable tree. Users who use MySQL in an untrusted multi-user environment should consider upgrading to this version, which also fixes a bug that enabled valid local users to crash mysqld by using a specially modified mysql client application.

### D.3.2 Changes in release 3.23.55 (23 Jan 2003)

- Fixed double free'd pointer bug in `mysql_change_user()` handling, that enabled a specially hacked version of MySQL client to crash mysqld. Note, that one needs to login to the server by using a valid user account to be able to exploit this bug.
- Fixed bug with the `--slow-log` when logging an administrator command (like `FLUSH TABLES`).
- Fixed bug in `GROUP BY` when used on `BLOB` column with `NULL` values.
- Fixed a bug in handling `NULLs` in `CASE ... WHEN ...`
- Bugfix for `--chroot` (see section D.3.3 Changes in release 3.23.54 (05 Dec 2002)) is reverted. Unfortunately, there is no way to make it to work, without introducing backward-incompatible changes in ``my.cnf'`. Those who need `--chroot` functionality, should upgrade to MySQL 4.0. (The fix in the 4.0 branch did not break backward-compatibility).
- Make `--lower-case-table-names` default on MacOSX as the file system is case insensitive.
- Fixed a bug in ``scripts/mysqld_safe.sh'` in `NOHUP_NICENESS` testing.
- Transactions in `AUTOCOMMIT=0` mode didn't rotate binary log.
- Fixed a bug in `scripts/make_binary_distribution` that resulted in a remaining `@HOSTNAME@` variable instead of replacing it with the correct path to the hostname binary.
- Fixed a very unlikely bug that could cause `SHOW PROCESSLIST` to core dump in `pthread_mutex_unlock()` if a new thread was connecting.
- Forbid `SLAVE STOP` if the thread executing the query has locked tables. This removes a possible deadlock situation.



MySQL 3.23.55, a new version of the popular Open Source Database, has been released. It is now available in source and binary form for a number of platforms from our download pages at <http://www.mysql.com/downloads/> and mirror sites.

Note that not all mirror sites may be up to date at this point of time - if you can't find this version on some mirror, please try again later or choose another download site.

This is a bugfix release for the current stable tree. Users who use MySQL in an untrusted multi-user environment should consider upgrading to this version, which also fixes a bug that enabled valid local users to crash mysqld by using a specially modified mysql client application.

#### D.3.2 Changes in release 3.23.55 (23 Jan 2003)

- Fixed double free'd pointer bug in `mysql_change_user()` handling, that enabled a specially hacked version of MySQL client to crash mysqld. Note, that one needs to login to the server by using a valid user account to be able to exploit this bug.
- Fixed bug with the `--slow-log` when logging an administrator command (like `FLUSH TABLES`).
- Fixed bug in `GROUP BY` when used on `BLOB` column with `NULL` values.
- Fixed a bug in handling `NULLs` in `CASE ... WHEN ...`
- Bugfix for `--chroot` (see section D.3.3 Changes in release 3.23.54 (05 Dec 2002)) is reverted. Unfortunately, there is no way to make it to work, without introducing backward-incompatible changes in ``my.cnf'`. Those who need `--chroot` functionality, should upgrade to MySQL 4.0. (The fix in the 4.0 branch did not break backward-compatibility).
- Make `--lower-case-table-names` default on MacOSX as the file system is case insensitive.
- Fixed a bug in ``scripts/mysqld_safe.sh'` in `NOHUP_NICENESS` testing.
- Transactions in `AUTOCOMMIT=0` mode didn't rotate binary log.
- Fixed a bug in `scripts/make_binary_distribution` that resulted in a remaining `@HOSTNAME@` variable instead of replacing it with the correct path to the hostname binary.
- Fixed a very unlikely bug that could cause `SHOW PROCESSLIST` to core dump in `pthread_mutex_unlock()` if a new thread was connecting.
- Forbid `SLAVE STOP` if the thread executing the query has locked tables. This removes a possible deadlock situation.