Firebird® Version 1.5.3 Release Candidate 2

Point Release Notes v.153_02
26 September 2005

The Firebird 1.5.3 sub-release introduces a number of retrospective fixes to bugs that became apparent and were fixed in the Firebird 2 tree during the pre-alpha and alpha phases of the Firebird 2 development. For now, these notes are a record of the changes. They should not be used in place of the main v.1.5 document.

Once the sub-release is done, the notes from sub-releases 1.5.1, 1.5.2 and this one will be merged as a single addendum to the main release notes.

Release Candidate 2

R E G R E S S I O N S F I X E D

ISSUE	**SF Bug # Fixed by**
Comparisons between strings in character set NONE and another character set would cause an error.	V. 1.5.2 regression
Solution Fixed.	D. Yemanov

B U G S F I X E D

ISSUE	SF Bug # Fixed by
Previously, a user could log into a server on a Unix/ Linux host remotely, using a Linux UID and password accepted on that host. It was recognised as a security hole and fixed in Firebird 2 development.	Endemic security bug
Solution Security fix backported: a UID received from the client side is now not trusted.	A. Peshkov
The isc_user_* (add/modify/delete) functions worked wrongly under Administrator account on Win32.	Unregistered bug
Solution At some point during InterBase development, the intention was to make the Win32 implementation work so that Superuser privileges on Unix were emulated for Administrator on Win32 (SuperUser/ root on Unix/Linux can log into the security database without entering any username and password). It worked, up to a point. However, if the Win32 Administrator user tried to call these functions through a SYSDBA login, the connection would hang with some strange path resolution errors. The code for a root-style login has been disabled in the Win32 clients (fbclient.dll and fbembed.dll).	A. Peshkov
Denial-of-Service vulnerability: an extra-long database file name could crash the server.	Endemic security bug
Solution One of many overflow vulnerabilities fixed in the Firebird 2 code, this fix has been backported to v.1.5.3.	A. Peshkov

Compound index key mangling exhibited a bug.	# 1242982
Solution Fixed.	A. Brinkman

A locally exploitable stack overflow vulnerability was detected.	# 739480
Solution Fixed.	A. Peshkov

Unnecessary evaluation was being performed on the last argument of the COALESCE function.	Unregistered bug
Solution Fixed.	A. Brinkman

Using search parameters in a SUM() operation would return incorrect results	# 1016969
Solution Fixed.	A. Brinkman

UPDATE with a CASE expression involving parameters would throw an SQLCode -804 exception ("Data type unknown").	# 1016969
Solution Fixed.	A. Brinkman

COALESCE/CASE displayed a bug regarding BLOB sub-type.	Unregistered bug
Solution Fixed.	A. Brinkman

There was an issue with quoted identifiers in the ISQL command SHOW GENERATORS in Dialect 3.	Unregistered bug
Solution Fixed.	C. Valderrama

M I N O R E N H A N C E M E N T S

ISSUE	SF Bug # Fixed by
Security diagnostics added.	N/A
Solution Attempts to send signals via a missing gds_relay may be an exploit attempt. They are now logged.	A. Peshkov

Release Candidate 1

R E G R E S S I O N S F I X E D

ISSUE	SF Bug # Fixed by
The wrong error was being detected when a write failure occurred.	v.1.5 Regression (not logged)
Solution Fix backported from Firebird 2 HEAD.	V. Horsun
An access violation could occur in fcblient.dll v1.5.2 on disconnecting.	v.1.5.2 Regression #1106825
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov
Generators were being initialized with garbage values on restoring from a metadata-only backup.	v.1.5.1 regression
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

B U G S F I X E D

ISSUE	SF Bug # / Fixed by
CPU load would rise to 100% when a write failure occurred.	Not logged
Solution Fix backported from Firebird 2 HEAD.	V. Horsun
A source of possible corruption was exhibiting in the Classic server as a page type exception "page 0 is of wrong type (expected 6, found 1)".	# 1076858
Solution Identified, fixed and backported from Firebird 2 HEAD.	V. Horsun
When the gfix service code tried to reattach to a database that had become unavailable, the server would crash.	Not logged
Solution An endless loop would occur due to the inability of the service to interact with the end user, causing the service buffer to overflow eventually and result in the crash. Fixed and backported from Firebird 2 HEAD.	V. Horsun
Character set and/or collation specified for local variables in PSQL would get lost, potentially causing string conversion errors	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov
If any DDL operations were active during a database shutdown, the server would crash.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

Subqueries in in VIEWs were returning character data with the wrong character set.	# 1110717
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

The server could crash while performing a metadata scan for a complex table.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

Database corruption could occur due to allowing certain pre-trigger actions, such as deleting a record in a BEFORE UPDATE trigger.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

User savepoints were not geing released when commit retaining was issued.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

Backport isql fixes from Firebird 2 HEAD	Unregistered bug
Solution	C. Valderrama

- Another fix for the -b (Bail On Error) option when SQL commands are issued and no database connection yet existed.
- Applied Miroslav Penchev's patch for a bug discovered by Ivan Prenosil, where the -Q switch would always return 1 to the operating system.
- Fixed a conflict between single-line and block comments.

If a table contained a computed column of BLOB or ARRAY type, the first column of the table could be zeroed during a restore.	Unregistered bug

Solution Fix backported from Firebird 2 HEAD.	D. Yemanov

In some cases, a BLOB filter declaration would cause the server to crash.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	C. Valderrama

The server would lock up if a request to attach to security.fdb was unsuccessful.	Unregistered bug , from v.1.5.0
Solution Fix backported from Firebird 2 HEAD.	C. Valderrama, D. Yemanov

---

The fbudf function AddMonth() exhibited wrong behaviour when facing January.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	C. Valderrama

The "FOR EXECUTE STATEMENT ... DO SUSPEND" construct in PSQL was exhibiting problems.	# 1124720
Solution Fix backported from Firebird 2 HEAD.	A. Peshkov

Bugchecks were being exhibited on AMD64 (and possibly other platforms) when a database was copied, rather than migrated using backup/restore.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	N. Samofatov

The server would crash during some DDL operations.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	A. Peshkov

There were issues with descending indices used in referential constraints.	Unregistered bug
Solution Fix backported from Firebird 2 HEAD.	A. Peshkov

An equality search on the first segment of a compound index, if it was an integer type, would result in redundant additional scans on specific values (2^n, e.g. 131072).	# 1242982
Solution Fix backported from Firebird 2 HEAD.	A. Brinkman

M I N O R E N H A N C E M E N T S

ISSUE	SF Bug # Fixed by
ISQL improvements	n/a
Solution • Command line switch -b to bail out on error when used in non-interactive mode. • Return an error code to the operating system from command-line isql	C. Valderrama, D. Ivanov

---