Firebird 2 Bug Fixes

Helen Borrie (Collator/Editor)

15 June 2009 - Document v. bf213_01 - for Firebird 2.1.3 & 2.0.5

Table of Contents

Firebird 2.1.x

Firebird 2.1.3

The following bug fixes/reversions have been applied since the release of v.2.1.2:

Core Engine

(CORE-2475) In Classic, external table data was visible only to the session that had operated on it.

fixed by V. Khorsun

(CORE-2449) An unexpected “lock conflict” error could be thrown instead of the appropriate exception.

fixed by D. Yemanov

(CORE-2444) The engine could hang when too many attachments were registering their interest in events simultaneously and exhausting free space in the events table.

fixed by V. Khorsun

(CORE-2441) The server could crash on executing an 'UPDATE OR INSERT' statement.

fixed by A. Peshkov

(CORE-2416) Preparing a query with aggregation over a derived table could cause an access violation.

fixed by V. Khorsun

(CORE-2415) Firebird would crash when temporary space was exhausted.

fixed by A. Peshkov

(CORE-2397) Database corruption could occur if two different indexes on a table were dropped within the same transaction.

fixed by V. Khorsun

(CORE-2355) LOWER() and UPPER() functions would misbehave when the byte length of the result was smaller than the input string.

fixed by A. dos Santos Fernandes

(CORE-2348) Problems with transaction numbers overflowing 32-bit signed integer and corrupting databases were appearing again.

fixed by V. Khorsun

(CORE-2340) Bugcheck 258 (page slot not empty) could occur under high concurrent load.

fixed by V. Khorsun

(CORE-2320) Complex recursive queries might not produce all rows.

fixed by V. Khorsun

(CORE-2311) A memory leak was possible in a WITH RECURSIVE query.

fixed by V. Khorsun

(CORE-2306) Superserver would terminate abnormally when a thread start failed.

fixed by A. Peshkov

(CORE-2291) Bugcheck 284 (cannot restore singleton select data) would occur in PSQL code involving some subqueries.

fixed by V. Khorsun

(CORE-1961) Bugcheck 210 (page in use during flush) was being thrown during database validation.

fixed by D. Yemanov, R. Simakov

(CORE-1690) Arithmetic exception, numeric overflow, or string truncation in UTF8 tables.

fixed by A. dos Santos Fernandes

(CORE-1647) The file associated with an external table needed to be closed after use, even if it was still apparently in use by some cached (inactive) requests.

fixed by V. Khorsun

Optimizer

(CORE-2411) The optimizer was choosing slower plans in v.2.0.5 and v2.1.2 than it would for the same queries in v.2.0.4 and v.2.1.1.

fixed by D. Yemanov

(CORE-1607) A correlated subquery that depended on the UNION stream would be optimized poorly.

fixed by D. Yemanov

Database Monitoring

(CORE-2483) The database permanent pool could get corrupted when working with monitoring tables.

fixed by D. Yemanov

(CORE-2482) Monitoring tables data collection could become unstable when attaching to or detaching from database.

fixed by A. Peshkov

Remote Interface

(CORE-2368) An isc_cancel_events() call would be succeeded by an access violation if the event was not found.

fixed by V. Khorsun

(CORE-2437) A buffer overflow could occur on a client during delivery of events.

fixed by A. Peshkov

(CORE-2313) A boundary condition could cause INF_* functions to invalidate the whole output buffer with *isc_info_truncated* at the beginning.

fixed by C. Valderrama

(CORE-2272) The server would start returning garbage when killing an attempt by an event to connect.

fixed by A. Peshkov

Windows-Specific

(CORE-1923) “instsvc remove” would return 1 (failure), even when execution was successful.

fixed by D. Yemanov

POSIX-Specific

(CORE-2249) Error while building Firebird 2.1 on FreeBSD 7.0.

fixed by A. Peshkov

(CORE-2247) On RISC platforms, message and descriptor buffers were not aligned properly.

fixed by A. Peshkov

Command-line Utilities

gbak

(CORE-2245) Error on restoring a database with long exception texts from backup.

fixed by C. Valderrama

isql

(CORE-2270) ISQL consumes all memory and crashes when running in zlogin console.

fixed by J. Swierczynski, A. Peshkov

fb_lock_print

(CORE-2354) "fb_lock_print -ia" output was not being flushed to a file between iterations.

fixed by A. Peshkov

User-defined Functions

(CORE-2282) **truncate* UDFs were broken for numbers smaller than -1.

fixed by C. Valderrama

(CORE-2281) **round* UDFs were broken for negative numbers.

fixed by C. Valderrama

Firebird 2.1.2

The following bug fixes/reversions have been applied since the release of v.2.1.1:

Core Engine

(CORE-2329) Discovered a significant source of performance degradation in comparison with V.1.5.

fixed by D. Yemanov

~ ~ ~

(CORE-2326) Committing a new user object (a view, for example) caused an access violation if a user-defined trigger had been applied to the system table RDB$RELATIONS.

It should be noted that no Firebird server version either supports, or retains after a backup and restore, any user-defined trigger on a system table. The strong recommendation against defining such triggers remains. The fix recognises one way that user interference with system tables can compromise internal operations and disarms it.

The ability to define "DDL triggers" through the regular DDL mechanisms is on the drawing board for V.3.

fixed by D. Yemanov

~ ~ ~

(CORE-2242) The engine was incorrectly populating integer containers in the blob parameter buffer (BPB) with integers in machine-local format, causing errors on Big Endian platforms.

fixed by A. Peshkov

~ ~ ~

(CORE-2241) If an ALTER TABLE ALTER COLUMN.. operation was performed on a table in the course of a bulk insert operation, minor index corruption could occur causing subsequent queries to return the wrong number of records. The bug was traced to legacy code in BTR\compress_root().

fixed by V. Khorsun

~ ~ ~

(CORE-2227) Problems were occurring in some environments when creating triggers that referred to column names with accented characters.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-2222) Storing a text blob with a transliteration blob filter could cause an access violation in the engine.

fixed by V. Khorsun

~ ~ ~

(CORE-2184) Superserver could hang when multiple clients were creating tables simultaneously.

fixed by D. Yemanov

~ ~ ~

(CORE-2182) It was not possible to drop an existing UDF whose name was duplicated by the name of a new built-in function.

fixed by D. Yemanov

~ ~ ~

(CORE-2173) The server would crash after an abnormal disconnection if there was an open ExecuteStatement call.

fixed by A. Peshkov

~ ~ ~

(CORE-2151) When a temporary directory path had spaces within it, it was (wrongly) being truncated at the rightmost space.

fixed by V. Khorsun

~ ~ ~

(CORE-2137) A database restore could crash the server when the configuration parameter *DummyPacketInterval* was set explicitly.

fixed by D. Yemanov

~ ~ ~

(CORE-2098) A bug in the implementation of Global Temporary Tables (GTT) allowed a GTT to be referred to in COMPUTED BY field expression. Since GTTs do not store global *data*, such an attempt should have been before the engine could attempt to store dependency records for the expression.

fixed by V. Khorsun

~ ~ ~

(CORE-2045) A regression occurred at v.2.1, whereby references to non-existent system fields with `blr_field` were not being resolved to NULL, whereas a parallel change involving `blr_fld` was exhibiting the proper corrective behaviour.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-2039) Domain-level CHECK constraints were (wrongly) processing NULLs as “zero values”, i.e. null dates as “date zero” (1858-11-17), null numerics as zero, null strings as empty strings, etc.

fixed by D. Yemanov

~ ~ ~

(CORE-2031) The first record output from a query with a search condition on RDB$DB_KEY was being returned with NULL in the first column.

fixed by A. A. dos Santos Fernandes

~ ~ ~

(CORE-2026) Temporary BLOBs (including implicit ones created when transliterating text from the BLOB character set to the connection one) could not be created while accessing a read-only database.

fixed by V. Khorsun

~ ~ ~

(CORE-2008) Procedure parameters that were declared NOT NULL were nevertheless being stored as nullable in RDB$PROCEDURE_PARAMETERS.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-2000) Under high load conditions, the lock manager could report false deadlocks.

fixed by V. Horsun

~ ~ ~

(CORE-1984) Lock manager would report false deadlocks if one of the deadlock participants was in WAIT with a permitted timeout.

fixed by V. Horsun

~ ~ ~

(CORE-1970) A “Lock conversion denied (bugcheck 215)” error could occur. This fix is related to CORE-1984 and CORE-2000 (above).

fixed by V. Horsun

~ ~ ~

(CORE-1963) A server could crash on commit when privileges were being granted or revoked simultaneously from multiple connections.

fixed by D. Yemanov

~ ~ ~

(CORE-1958) When attempting to update the same record multiple times, a "Bugcheck 179 (decompression overran buffer)" failure could occur.

fixed by D. Yemanov

~ ~ ~

(CORE-1930) In a situation where a stored procedure was altered to remove output parameters and dependent procedures are not recompiled, the engine should properly track the dependencies and return an exception when the altered procedure is called. Instead, it was crashing.

fixed by V. Horsun

~ ~ ~

(CORE-1506) The server would crash with `isc_dsql_execute_immediate` and a zero-length string.

fixed by A. Peshkov

~ ~ ~

(CORE-1596) There was a length-related bug in CsConvert::convert that had to be revisited.

fixed by A. dos Santos Fernandes

~ ~ ~

Services API

(CORE-1982) Simultaneous backups or restores using the Services API under Superserver could interfere with one another.

fixed by A. dos Santos Fernandes

~ ~ ~

Database Monitoring

(CORE-2209) Monitoring requests in high load conditions could become very slow and even block other activity during that time.

fixed by D. Yemanov

~ ~ ~

(CORE-2171) The column MON$CALLER_ID of table MON$CALL_STACK was reporting invalid IDs.

fixed by D. Yemanov

~ ~ ~

(CORE-2017) Monitoring tables were not keeping account of I/O statistics for stored procedures.

fixed by D. Yemanov

~ ~ ~

(CORE-1944) Monitoring tables contained wrong data on big-endian machines.

fixed by A. Peshkov

~ ~ ~

(CORE-1926) MON$DATABASE was returning outdated transaction counters.

fixed by D. Yemanov

~ ~ ~

Optimizer

(CORE-2078) The optimizer always had some trivial heuristics to estimate the effective stream selectivity, even if no indices could be used for the retrieval. This code missed being migrated into the ODS11 optimizer logic. The effect was that join orders chosen for cases involving non-indexed predicates were likely to be ineffective.

fixed by D. Yemanov

~ ~ ~

(CORE-2053) Computed expressions may be optimized badly if used inside the RETURNING clause of the INSERT statement

fixed by D. Yemanov

~ ~ ~

Database Manipulation Language (DML)

(CORE-2073) The implementation of expression indexes exhibited a bug whereby an incorrect result was returned when an inverted Boolean predicate was applied to test an indexed expression.

fixed by D. Yemanov

~ ~ ~

(CORE-2118) With an UPDATE OR INSERT statement, an insert would fail silently if the MATCHING operand was a subquery.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1962) Incorrect extraction of MILLISECONDs:

```
select extract(millisecond from time '01:00:10.1234')
from rdb$database
```

would return 10123 instead of 123.4.

fixed by A. dos Santos Fernandes

~ ~ ~

Procedural Language (PSQL)

(CORE-2117) Incorrect ROW_COUNT values were being returned with indexed retrieval and subqueries.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1919) Memory corruptions in EXECUTE STATEMENT could crash the server.

fixed by A. dos Santos Fernandes

~ ~ ~

Security

(CORE-2087) When the configuration parameter *RemoteBindAddress* specified a hostname instead of an IP address, or specified a non-existent IP address, it would be silently ignored and the server would bind to all interfaces, without any notification in firebird.log or the system log. This was considered a potential security risk if the system had ports open to the Internet. Now, an invalid or unavailable IP address will be resolved to localhost (127.0.0.1).

fixed by A. Peshkov

~ ~ ~

(CORE-2084) Services API security problem, specific to Firebird 2.1: services would ignore the setting of the *Authentication* parameter in firebird.conf. Once a user was logged, any server-level operations not requiring a further login, such as viewing the firebird.log file or getting information about the server, etc., were accessible by any valid domain user.

fixed by A. Peshkov

~ ~ ~

(CORE-2055) Backported a fix for a known buffer overflow in the Firebird client library.

fixed by A. Peshkov

~ ~ ~

(CORE-1972) A non-SYSDBA user was able to change the Forced Writes mode of any database, along with several other database characteristics that should be restricted to the SYSDBA. This long-standing, legacy

loophole in the handling of DPB parameters could lead to database corruptions or give ordinary users access to SYSDBA-only operations. The changes could affect several existing applications, database tools and connectivity layers (drivers, components). Details are in Chapter 3 of the V.2.1.2 Release Notes, in *Changes to the Firebird API and ODS*.

fixed by A. Peshkov

~ ~ ~

(CORE-1957) Because of a change done in the conversion to C++ at v.1.5, ACLs (Access Control Lists) longer than about 20 characters were being truncated. This has caused particular problems for applications that construct access privileges in run-time and has also given rise to privileges “going missing” when there are more than about 2000 privileges (for a report of the latter, see Tracker issue CORE-216).

fixed by A. Peshkov

~ ~ ~

(CORE-1922) Trusted authentication would not work with the Services API.

fixed by A. Peshkov

~ ~ ~

Utilities

gfix Houskeeping Toolset

(CORE-2271) The *gfix* utility had a legacy bug that exhibited itself during the database validation/repair routines on large databases. The privilege level of the user running these routines was being checked too late in the operation, thus allowing a non-privileged user (i.e., not SYSDBA or Owner) to start a validation operation. Once the privilege check occurred, the database validation could halt in mid-operation and thus be left unfinished, resulting in logical corruption that might not have been there otherwise.

fixed by A. Peshkov

~ ~ ~

nBackup Incremental Backup Utility

(CORE-2266) nBackup's database locking was not working correctly, causing database file growth to continue when database writes should have been in suspension.

fixed by V. Khorsun

~ ~ ~

gbak Backup and Restore Utility

(CORE-2223) gbak was encountering several bugs when operating on the access control lists (ACLs) that store SQL privileges.

fixed by A. Peshkov

~ ~ ~

(CORE-1843) Paths with spaces were being refused by gbak when it was called with the -se[rvice_mgr] switch.

fixed by A. Peshkov

~ ~ ~

POSIX-specific

(CORE-2221) On POSIX platforms, any attachment to any database would fail after the access rights for security2.fdb were modified from 0660 to 0666.

fixed by P. Beach, A. Peshkov

~ ~ ~

(CORE-2157) Known issue: a bug in gcc 3.2.x, the compiler used to build the official x86 Linux packages, can cause problems when people try to build binaries that depend on the Firebird client without using the -pthread switch. Setting the -pthread switch removes the dependency of the output binary on libpthread.

Reported by A. Peshkov

~ ~ ~

(CORE-2077) On POSIX platforms, the Classic server in embedded mode, i.e., loaded into the user's application space, would handle the TERM signal but would fail to call any other signal handlers in the queue. The effect was that signal handlers set by the application were not executed and the application would keep working after the termination. It was a bad idea to invoke `ISC_signal_cancel()` from the signal handler and the mechanism has been reworked.

fixed by A. Peshkov

~ ~ ~

(CORE-2050) Fixed a performance regression resulting from a surfeit of `semop()` system calls.

fixed by V. Horsun

~ ~ ~

(CORE-2049) Fixed a performance regression resulting from a surfeit of `sigprocmask()` system calls.

fixed by A. Peshkov

~ ~ ~

(CORE-2033) The symbol _Unwind_GetIP in the client library was being left unresolved due to a missing static library linkage.

fixed by A. Peshkov

~ ~ ~

(CORE-1983) In any POSIX environment except Solaris, the engine was mishandling the “out of memory” condition, causing the server to crash.

fixed by A. Peshkov

~ ~ ~

(CORE-1909) Garbage text was being printed to firebird.log on AMD64 Linux.

fixed by A. Peshkov

~ ~ ~

(CORE-2093) Superserver startup was failing on Solaris 64-bit.

fixed by A. Peshkov

~ ~ ~

Windows-specific

(CORE-2234) Sometimes, terminated worker processes in Classic on Windows were still considered to be alive after termination, due to improper checks on the Firebird server's part. The same bug could cause the Firebird server to misbehave with prolonged deadlocks when under load.

fixed by D. Yemanov

~ ~ ~

(CORE-2108) When using the new implementation of Windows local protocol (XNET), the next available map number was calculated incorrectly, thus allowing the server to try to reuse a map number that already existed. If the “new” map's timestamp was equal to the timestamp of the pre-existing map, it would cause the `get_free_slot()` function to fail.

fixed by V. Khorsun

~ ~ ~

MacOSX-specific

Unregistered bug When Firebird is configured to run in some specific directory (/usr/local/firebird, /opt/firebird or any other) the @prefix@ macro should be substituted with that directory path. On MacOS it was not done and caused exceptions to be thrown when the engine tried to locate some of its components.

fixed by P. Beach

~ ~ ~

(CORE-2065) The MacOSX installation package was in violation of platform rules by not including the client library in the dynamic loader search paths.

fixed by P. Beach

~ ~ ~

Firebird 2.1.1

The following bug fixes/reversions have been applied since the release of v.2.1:

Database Monitoring

(CORE-1890) The database monitoring process could hang under high load.

fixed by D. Yemanov, V. Khorsun

~ ~ ~

(CORE-1881) Database monitoring could crash the server or mess up its page-locking logic.

fixed by D. Yemanov

~ ~ ~

Build/Installer Issues

(CORE-1889) Builds were creating the security database with Forced Writes OFF in all Firebird versions, allowing the possibility of corruption in unstable environments. From 2.1. 1 onward, builds will create security2.fdb with FW ON.

Improvement implemented by A. Peshkoff

~ ~ ~

(CORE-1826) The *changeRunUser.sh* and *restoreRootRunUser.sh* scripts were not changing the run user in *init.d* scripts.

fixed by A. Peshkoff

~ ~ ~

Security Issues

(CORE-1887) New databases were being created with the wrong access privileges.

fixed by A. Peshkoff

~ ~ ~

(CORE-1854) The value of CURRENT_USER was not always being converted to upper case when using operating system authentication on POSIX.

fixed by A. Peshkoff

~ ~ ~

(CORE-1845) Some standard calls would show the server installation directory to regular users.

fixed by A. Peshkoff

~ ~ ~

Character Set/Collation Issues

(CORE-1885) Processing a CREATE COLLATION statement on POSIX 64-bit versions would cause the server to crash.

fixed by A. dos Santos Fernandes, A. Peshkov

~ ~ ~

(CORE-1802) Wrong maximum key size was being calculated when the collation used was PXW_CSY.

fixed by A. dos Santos Fernandes

~ ~ ~

Procedural Language (PSQL)

(CORE-1884) Random crashes could occur when using stored procedures that were defined with input parameters having expressions as the default value.

fixed by V. Khorsun

~ ~ ~

Utility Programs

(CORE-1876)

*fixed by N. Samofatov*The nbackup incremental backup utility was broken.

~ ~ ~

(CORE-1875) An isql script that accessed CURRENT_DATE could throw an error or crash the server.

fixed by V. Khorsun

~ ~ ~

(CORE-1864) In isql on big-endian hosts, the SELECT operator did not work.

fixed by A. Peshkoff, P. Beach

~ ~ ~

Dynamic SQL (DSQL)

(CORE-1868) The server could crash in *isc_dsql_free_statement()*.

fixed by A. Peshkoff

~ ~ ~

(CORE-1859) "Arithmetic overflow or division by zero" errors were occurring while processing calls to the MAX() function.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1839) The server could crash when sorting on a field that was calculated using a recursive common table expression (CTE).

fixed by A. Peshkoff

~ ~ ~

(CORE-1798) RDB$DB_KEY was evaluated as NULL in INSERT ... RETURNING

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1793) On preparing a parameterised CTE with unused parameters, the server would crash.

fixed by V. Khorsun

~ ~ ~

(CORE-1781) LIKE, STARTING WITH and CONTAINING could return false positives.

fixed by A. dos Santos Fernandes

~ ~ ~

Engine Issues

(CORE-1851) Windows applications using *fbembed.dll* could hang during the process termination if there were open connections.

fixed by D. Yemanov

~ ~ ~

(CORE-1844) The Valgrind tools were frequently reporting the error "Conditional jump or move depends on uninitialised value(s)" in the function *check_status_vector()*.

fixed by A. Peshkoff

~ ~ ~

(CORE-1841) A view using derived table names or aliases that were too long could cause RDB $VIEW_RELATIONS.RDB$CONTEXT_NAME to overflow.

fixed by V. Khorsun

~ ~ ~

(CORE-1840) Each DDL execution was producing a small memory leak.

fixed by D. Yemanov

~ ~ ~

(CORE-1838) SET STATISTICS *INDEX* on an index of a global temporary table (GTT) could wrongly change the index ID by an amount equivalent to the maximum available number for the database page size.

fixed by V. Khorsun

~ ~ ~

(CORE-1830) Index corruption was possible when multiple updates of the same record were performed in the same transaction with savepoints in use.

fixed by V. Khorsun

~ ~ ~

(CORE-1819) A more efficient solution was implemented for a bug that had caused lower-level index pages to be missed in indirection from the parent page (replacing the original fix for CORE-1300).

fixed by V. Khorsun

~ ~ ~

(CORE-1812) Indexes were being overlooked for some date/time expressions in dialect 1.

fixed by D. Yemanov

~ ~ ~

(CORE-1807) On POSIX, the fbserver process was getting assigned to a random, non-canonical port after an abnormal termination.

fixed by A. Peshkoff

~ ~ ~

(CORE-1731) The engine would sometimes engine hang for several minutes, using 100% CPU load, with no sign of I/O activity.

fixed by V. Khorsun

~ ~ ~

(CORE-1421) Superserver failed to shut down immediately after a shutdown request if the request was preceded by a failed login attempt.

fixed by A. Peshkoff

~ ~ ~

Miscellaneous

(CORE-1817) The *RelaxedAliasChecking* parameter was having no effect on the RDB$DB_KEY field

fixed by V. Khorsun

~ ~ ~

(CORE-1810)

*fixed by A. Peshkoff*There was an issue with user names containing the '.' character.

~ ~ ~

(CORE-1775) The performance of security class checking during prepares was poor compared with v.1.5.x.

fixed by V. Khorsun

~ ~ ~

(CORE-1357) The DummyPacketInterval mechanism was broken.

fixed by D. Yemanov

~ ~ ~

Firebird 2.1 Post-RC2 Fix

The following bug in the Windows builds was detected during field-testing of release candidate 2 and was fixed before QA of the final release build. The same bug affects Firebird 2.0.3 and all of the Firebird 1.5.x series:

(CORE-1820) The Windows server executables failed to return a meaningful response when the Windows installer script queried to detect a running server. Thus, if an install was actually being performed while an existing server was running, the query would return a false negative and the install would continue instead of aborting, causing the potential for either installation to be corrupted or inconsistent.

> **Tip**
>
> It is always advisable to shut down a running server before attempting an install, in any event!

The Windows server program now delivers the correct signal in response to the installer's query.

fixed by D. Yemanov, P. Reeves

~ ~ ~

Firebird 2.1 Release Candidate 2

The following bug fixes/reversions have been applied since RC 1:

Data Manipulation Language (DML)

(CORE-1713) Legacy behaviour of SELECT DISTINCT * on a table structure containing BLOB columns has been reverted and, along with it, the legacy behaviours when UNION, GROUP BY and ORDER BY operations refer to BLOB columns.

> **Warning**
>
> Be aware that the result sets produced may be incorrect, due to ordering and distinction being performed on the BLOB_ID, not on contents of the BLOB.

Earlier changes CORE-859 and CORE-1530 are thus also implicitly rolled back.

fixed by D. Yemanov

~ ~ ~

(CORE-1724) Common table expressions could not be used in computed columns and quantified predicates (IN / ANY / ALL). Now the behaviour of CTEs in SELECTS is aligned with that of other virtual table types.

fixed by V. Khorsun

~ ~ ~

(CORE-1716) Variable initialization in recursive procedures was being performed wrongly.

fixed by A. dos Santos Fernandes

~ ~ ~

Server Crashes

(CORE-1729) The server process would terminate when selecting the MON$ data was attempted in a system with a heavy load of concurrent connections.

fixed by D. Yemanov

~ ~ ~

POSIX-specific

(CORE-1818) Temporary files used for temporary page spaces were not being deleted after use on POSIX platforms.

fixed by A. Peshkov

~ ~ ~

(CORE-1728) After a fresh Linux install, monitoring tables would be found to be not working.

fixed by A. Peshkov

~ ~ ~

Services Manager

(CORE-1726) Failure was exhibited in *isc_service_start()*.

fixed by A. Peshkov

~ ~ ~

Data Definition Language (DDL)

(CORE-1746) It was (wrongly) possible to create an expression index while inserts into the table were under way.

fixed by V. Khorsun

~ ~ ~

(CORE-1715) A “key size exceeds implementation restriction for index” exception was being wrongly returned under some conditions.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1694) A bug was exhibited in creating or altering database triggers, related to attempts to include comment statements using a Russian character set.

fixed by A. dos Santos Fernandes

~ ~ ~

Firebird 2.1 Release Candidate 1

A number of internal optimizations were done by Alex Peshkov between Beta 2 and this release to reduce some areas of degradation in performance that had materialised as a side- effects of new feature implementations. Besides these, the following bug fixes/improvements have been applied since Beta 2:

Core Engine/DSQL

(CORE-1657) Memory access violations (segfaults) could occur where read-only read committed transactions were left idle for a long time in a system under heavy load.

fixed by A. Peshkov

~ ~ ~

(CORE-1648) RDB$TYPES was failing to list the types for database triggers.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1644) Compiling on GCC 4.1.1 was throwing a compilation error.

fixed by A. Peshkov

~ ~ ~

(CORE-1641) CREATE TRIGGER was causing two copies of the trigger object to exist in the metadata cache simultaneously.

fixed by D. Yemanov

~ ~ ~

(CORE-1624) MERGE worked incorrectly when there were parameters in a MATCHING clause

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1610) A full shutdown could cause database corruption.

fixed by D. Yemanov

~ ~ ~

(CORE-1597) It was (erroneously) possible to create global temporary tables in a database with an ODS lower than 11.1.

fixed by V. Khorsun

~ ~ ~

(CORE-1579) On 64-bit builds, a UDF that carried a BLOB as an argument could corrupt the BLOB on the stack by partly overwriting it if another argument was a string.

fixed by A. Peshkov

~ ~ ~

(CORE-1574) A number of problems appeared concerning multi-file databases.

fixed by V. Khorsun

~ ~ ~

(CORE-1562) Shutdown would fail to kill high-load query connections.

fixed by D. Yemanov

~ ~ ~

(CORE-1549) A performance-killer regression dating back to v.1.5 meant subquery-based predicates (IN, EXISTS, etc.) were not evaluated early enough in the join order to enable efficient filtering.

fixed by D. Yemanov

~ ~ ~

(CORE-1539) A transliteration error could occur in a SELECT statement on a system table, where the wildcard ('%') element of the search argument for 'LIKE' substituted metadata elements containing non-ASCII characters, e.g., in a CHECK constraint.

fixed by Adriano Dos Santos Fernandes

~ ~ ~

(CORE-1533) A JOIN on the first record of an ordered derived table would return the wrong record.

fixed by D. Yemanov

~ ~ ~

(CORE-1509) Extraneous trailing spaces were being inserted when casting DOUBLE PRECISION numbers to VARCHAR().

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1501) SLONG data in dsql_nod was being accessed wrongly.

fixed by A. Peshkov

~ ~ ~

(CORE-1500) Data in the internal buffer of EXECUTE STATEMENT was not being aligned correctly.

fixed by A. Peshkov

~ ~ ~

(CORE-1492) Compatibility between a text BLOB and a CHAR or VARCHAR was not working for COALESCE().

fixed by A. Dos Santos Fernandes

~ ~ ~

Server Crashes

(CORE-1681) Garbage data in the incoming remote packet could crash the server

fixed by D. Yemanov

~ ~ ~

(CORE-1649) Access violations could occur when a recursive query used the MERGE JOIN method in its execution plan.

fixed by V. Khorsun

~ ~ ~

(CORE-1601) The server could crash inside the page validation routine.

fixed by D. Yemanov

~ ~ ~

(CORE-1519) Memory access violations were occuring in isc_dsql_fetch().

fixed by V. Khorsun

~ ~ ~

(CORE-1199) Internal GDS software consistency check (CCH_precedence: block marked (212))

fixed by V. Khorsun

~ ~ ~

Linux-specific

(CORE-1589) The start-stop script for SuperServer on Linux sometimes failed to stop the service.

fixed by A. Peshkov

~ ~ ~

Windows-specific

(CORE-1602) Trusted authentication was not mapping domain administrators to the SYSDBA login.

fixed by D. Yemanov

~ ~ ~

(CORE-1593) Windows rules for full domain user names allow names longer than the 31 characters allowed by Firebird. Firebird was accepting such names via trusted authentication and failure was messy. Now, the 31-character limit is enforced and logins passing longer names are disabled. (This will remain the situation until the mapping of OS objects to database objects is implemented in a later Firebird version.)

fixed by A. Peshkov

~ ~ ~

(CORE-1543) A bug in the remote interface checking for trusted authentication was enabling any OS user to log in as SYSDBA.

fixed by A. Peshkov

~ ~ ~

Data Manipulation Language

Inbuilt Functions

(CORE-1677) Inbuilt functions FLOOR and CEILING returned wrong results with exact numeric arguments.

fixed by A. Dos Santos Fernandes

~ ~ ~

Improvement (CORE-1623) Inbuilt function HASH() needed improvement in its memory consumption when processing a BLOB argument.

fixed by A. Dos Santos Fernandes

~ ~ ~

Improvement (CORE-1569) The scale argument of the ROUND() function was made optional.

fixed by A. Dos Santos Fernandes

~ ~ ~

Improvement (CORE-1546) The "randomness" quality of the result from the RAND() function was improved.

fixed by A. Dos Santos Fernandes

~ ~ ~

Improvements (CORE-1490 and *CORE-1497)* The keywords used in the expanded forms of the DATEADD() and DATEDIFF() functions were changed to more meaningful words.

fixed by A. Dos Santos Fernandes

~ ~ ~

Improvement (CORE-1511) An optional argument was added to the expanded form of the POSITION() function to take a starting position offset.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1582) The inbuilt ABS() function was rounding values of NUMERIC data type.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1560) The inbuilt function NULLIF() would crash the server if the value passed to the first argument was an empty string constant ('').

fixed by A. Peshkov

~ ~ ~

(CORE-1528) The inbuilt functions DATEDIFF() and ABS(integer const) would not work in a dialect 1 database.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1522) The inbuilt function DATEDIFF() was exhibiting inconsistent behaviour.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1514) Many new 2.1 built-in functions exhibited incorrect NULL semantics.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1489) The inbuilt function DATEADD was not working properly with NULL arguments.

fixed by A. Dos Santos Fernandes

~ ~ ~

Remote Interface/API

(CORE-1679) **The isc_service_query()** function was returning garbage bytes in the output.

fixed by A. Peshkov

~ ~ ~

(CORE-1651) The client library could sometimes falsely report a request synchronization error (isc_req_sync) to a client application.

fixed by V. Khorsun

~ ~ ~

(CORE-1510) XSQLVAR [NULL flags] for (2*COALESCE(NULL,NULL)) were bad.

fixed by A. Dos Santos Fernandes, D. Kovalenko

~ ~ ~

International Language Support

(CORE-1594) An alignment issue in character set conversion could cause extraneous trailing spaces on some platforms. Code CsConvert::convert() was refactored slightly to address the issue.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1375) Wrong mapping for 0x212C in cs_gb2312.h

fixed by A. Dos Santos Fernandes

~ ~ ~

Database Monitoring/Administration

(CORE-1642) Monitoring under non-privileged login credentials would report wrong attachment data.

fixed by D. Yemanov

~ ~ ~

(CORE-1584) Inserting into monitoring tables could cause a crash or a bugcheck.

fixed by V. Khorsun

~ ~ ~

(CORE-1567) Regression behaviour exhibited in Beta 2 Embedded, where selecting from MON$STATEMENTS would yield an error and an exit() call.

fixed by D. Yemanov

~ ~ ~

(CORE-1561) Selecting from MON$STATEMENTS could cause the server to lock up.

fixed by D. Yemanov

~ ~ ~

(CORE-1551) A memory access violation would occur if all statements and all attachments were cancelled via the monitoring tables.

fixed by A. Peshkov

~ ~ ~

Security

(CORE-1603)

*fixed by A. Peshkov*A long user name was a potential source of buffer overflow.

~ ~ ~

Command-line Utilities

isql

(CORE-1493) When extracting a script, isql was not mangling BLOB filter and UDF information with embedded quotes properly.

fixed by C. Valderrama

~ ~ ~

gsec

(CORE-1680) **gsec display** would show only a few initial users when there were more than 50 users in the security database

fixed by A. Peshkov

~ ~ ~

(CORE-1637) A problem in the GSEC shell utility was causing the 'DISPLAY' command to (wrongly) return a SPB error.

fixed by A. Peshkov

~ ~ ~

gfix

(CORE-1548) Some errors in GFIX were returning wrong error codes, or not returning any error code.

fixed by A. Peshkov

~ ~ ~

(CORE-1481) False errors were likely to be reported by gfix when using in-memory metadata.

fixed by V. Khorsun

~ ~ ~

gbak

(CORE-1540) A fatal Lock Manager error would occur at the end of a gbak restore.

fixed by D. Yemanov

~ ~ ~

(CORE-374) Restore would fail on a table that had computed fields computed by selecting a value from a stored procedure.

fixed by N. Samofatov

~ ~ ~

nbackup

(CORE-1537) The nbackup utility would create its difference file for a database on a raw device in a bad 'default location'. For raw devices, nbackup needed to enforce a file system path for the difference file.

fixed by A. Peshkov

~ ~ ~

Firebird 2.1 Beta 2

The following section details the bug fixes that have been applied since the Beta 1 release:

Core Engine/DSQL

(CORE-1476) Forced writes have never actually worked on Linux, leaving open the potential for system trauma to break databases even with FW=ON. It has actually been known to happen on Linux.

fixed by A. Peshkov

~ ~ ~

(CORE-1468) Database corruption was possible when database file expansion and read\write activity were being performed simultaneously.

fixed by V. Khorsun

~ ~ ~

(CORE-1440) Transaction options were dangerously lacking in validation.

fixed by C. Valderrama

~ ~ ~

(CORE-1418) Rapidly starting and shutting down could cause a race condition in the blocking AST thread due to poor synchronization.

fixed by A. Peshkov

~ ~ ~

(CORE-1401) Instances of a global temporary table were not always picking up all indices.

fixed by V. Khorsun

~ ~ ~

(CORE-1361) Index operations for global temporary tables were not visible to the active connection.

fixed by V. Khorsun

~ ~ ~

(CORE-1380) Changing the Forced Writes setting for a database would cause I/O errors if the database had existing attachments.

fixed by V. Khorsun

~ ~ ~

(CORE-1408) UDF names using reserved words were being extracted with the double quotes missing.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1379) Invalid parameter type ("Data type unknown" error) when passing the argument to the CHAR_LENGTH function as a parameter.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1347) Unexpected "cannot transliterate" error.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1332) The SQLSCALE member of a text BLOB column can carry the BLOB's character set. In some documentation it wrongly says it should always be there. Text BLOBs needed to be brought into line with character types, i.e., if the connection character set is other than NONE and the BLOB's character set is not NONE or OCTETS, then it should be the character set of the connection.

fixed by A. dos Santos Fernandes

~ ~ ~

Server Crashes

(CORE-1470) The server would crash if a secondary file name was longer than 127 characters.

fixed by C. Valderrama

~ ~ ~

(CORE-1457) The server would crash when attempting to deliver events for a session that had just disconnected.

fixed by V. Khorsun, D. Yemanov

~ ~ ~

(CORE-1451) Using RDB$DB_KEY in the **WHERE** clause of a SELECT from a stored procedure would crash the server.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1338) Connection lost (error 335544721, Unable to complete network request to host ...) when selecting from a view having a derived field defined with ROUND().

fixed by D. Yemanov

~ ~ ~

(CORE-1334) Joins with a NULL RDB$DB_KEY would crash the server.

fixed by A. dos Santos Fernandes

~ ~ ~

Windows-Specific

(CORE-1456) Wrong events delivery could occur where there were concurrent XNET connections.

fixed by V. Khorsun, D. Yemanov

~ ~ ~

(CORE-1443) On 64-bit Windows 2003 Server, the embedded engine could cause an application to hang on exit if no database access was performed.

fixed by V. Khorsun

~ ~ ~

(CORE-1403) The server under Windows would crash if multiple events were being registered simultaneously by a client connected via the XNET protocol.

fixed by D. Yemanov

~ ~ ~

Data Definition Language (DDL)

(CORE-1395) CHECK constraints on domains were demonstrating a few problems.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1378) A number of issues were reported regarding domain names and character sets.

fixed by A. dos Santos Fernandes

~ ~ ~

Data Manipulation Language (DML)

(CORE-1466) The SUBSTRING() function could return a truncated substring for some multi-byte BLOBs.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1428) Timestamp subtraction in dialect 3 was incorrect if the calculation would result in a negative number.

fixed by V. Khorsun

~ ~ ~

(CORE-1417) Error “Invalid BLOB ID” error could occur when performing an insert using InterBaseXpress.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1373) A recursive CTE query would produce incorrect results when the recursive member's SELECT list contained an expression involving self-referencing fields.

fixed by V. Khorsun

~ ~ ~

Procedural Language (PSQL)

(CORE-1434) EXECUTE STATEMENT was truncating the last two bytes of VARCHAR columns.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1419) CURRENT_TIMESTAMP was being wrongly evaluated during the execution of selectable procedures.

fixed by D. Yemanov

~ ~ ~

(CORE-1371) An EXECUTE BLOCK sequence would fail if it was passed within an EXECUTE STATEMENT string.

fixed by A. Peshkov

~ ~ ~

(CORE-1370) Use of CTE within procedures was causing memory leaks.

fixed by V. Khorsun

~ ~ ~

(CORE-1331) Character set transliterations would not work with EXECUTE STATEMENT.

fixed by A. dos Santos Fernandes

~ ~ ~

Remote Interface

(CORE-1455) Crash in fbclient after an unsuccessful user management API call.

fixed by A. Peshkov

~ ~ ~

(CORE-1452) The client library would crash when attempting to process an event received just before disconnection. (Did not affect libfbembed.so.)

fixed by D. Yemanov, V. Khorsun

~ ~ ~

(CORE-1430) Access Violation in fbclient.dll if a statement was prepared and executed right after events were registered.

fixed by V. Khorsun

~ ~ ~

(CORE-1388) It was not possible to attach to the Service Manager remotely if the remote engine version was less than 2.0.

fixed by V. Khorsun

~ ~ ~

(CORE-1349) The remote interface was not validating the client-supplied message length against the message format length.

fixed by V. Khorsun

~ ~ ~

API

(CORE-1485) Fixed a very ancient bug whereby the **sqllen** field in the xsqlvar contained length of data in a varying structure, not its total size. In any OS environment it could cause an access violation when loading messages in msg.fdb

fixed by A. Peshkov

~ ~ ~

(CORE-1416) Incorrect parameter order in a TPB was being accepted without returning an error.

fixed by C. Valderrama

~ ~ ~

(CORE-1372) If **isc_dsql_fetch()** is called after **isc_commit_transaction()** an exception should be raised. That was not happening.

fixed by V. Khorsun

~ ~ ~

International Language Support (INTL)

(CORE-1484) INTL modules compiled in the Linux, gcc 4.1.2, amd64 environment would cause an access violation in Superserver, due to use of the standard operator **new** but the overloaded operator **delete**.

fixed by A. Peshkov

~ ~ ~

(CORE-1446) Problem with UNICODE collations from fbintl when using system ICU.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1431) There were some inherent issues with uppercasing certain Greek characters in cp1251.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1384) LIKE would not work correctly with collations using SPECIALS-FIRST=1.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1339) The metadata character set upgrade script was generating garbage in descriptions.

fixed by A. dos Santos Fernandes

~ ~ ~

Database Monitoring/Admin

(CORE-1467) A database attachment would go into some kind of invalid state after its long-running statement was canceled via MON$STATEMENTS, returning a 'database shutdown' error.

fixed by D. Yemanov

~ ~ ~

(CORE-1441) Query cancellation feature could not interrupt a long fetch.

fixed by D. Yemanov

~ ~ ~

(CORE-1436) Outer joins would not work properly with the MON$ tables.

fixed by D. Yemanov

~ ~ ~

(CORE-1359) The server would crash at the first operation with the monitoring tables if the filesystem lacked the necessary permissions for the shared-memory file.

fixed by D. Yemanov

~ ~ ~

(CORE-1358) Operations with MON$STATEMENTS were throwing "cannot transliterate" errors.

fixed by D. Yemanov

~ ~ ~

(CORE-1330) Semaphores were being double-locked when the monitoring tables were queried during long fetches.

fixed by D. Yemanov

~ ~ ~

Security

(CORE-1447) Querying for database info on very long path through an isc_database_info() API call could cause a buffer overrun.

fixed by C. Valderrama

~ ~ ~

(CORE-1397) A possible vulnerability was discovered in the remote server attachment.

fixed by V. Khorsun

~ ~ ~

(CORE-1312) A remote attacker could check for the presence of a file on a system running the Firebird server.

fixed by A. Peshkov

~ ~ ~

Command-line Utilities

gstat

(CORE-1400) GSTAT did not support infixing the port number in the connection string.

fixed by D. Yemanov

~ ~ ~

(CORE-1399) GSTAT would not use the RemoteServicePort configured in firebird.conf.

fixed by D. Yemanov

~ ~ ~

(CORE-1398) GSTAT was treating 'localhost' as case-sensitive in Windows.

fixed by D. Yemanov

~ ~ ~

gbak

(CORE-1369) Default values of procedure parameters were not being caught when downgrading a database from ODS11.1.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1344) Error "request depth exceeded" when restoring complex metadata.

fixed by D. Yemanov

~ ~ ~

isql

(CORE-1465) ISQL would ignore an explicit constraint name when it was confused with an internal, automatic name.

fixed by C. Valderrama

~ ~ ~

(CORE-1261) isql would ignore the index and ordering in a UNIQUE CONSTRAINT when generating a metadata script.

fixed by C. Valderrama

~ ~ ~

Firebird 2.1 Beta 1

The following are rough groupings to help you find specific bug fixes that you want to check up on. In general, expect these to be fixes that were deferred at the 2.0 release or showed up as regressions after a 2.0.x or 2.1 Alpha release.

Core Engine/DSQL

(CORE-1248) Incorrect timestamp arithmetic was performed when one of the operands was a negative number.

fixed by V. Khorsun

~ ~ ~

(CORE-1228) Reports of database corruption after an out-of-disk-space condition.

fixed by V. Khorsun

~ ~ ~

(CORE-1227) LIST() function would seem to fail if used twice or more in a query.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1215) Wrong SELECT query results using index to evaluate >= condition

fixed by V. Khorsun

~ ~ ~

(CORE-1175) Error “Data type unknown” when any UDF argument was a built-in function containing a DSQL parameter reference.

fixed by D. Yemanov

~ ~ ~

Server Crashes

(CORE-1244) Server crash on “select * from <recursive CTE>”.

fixed by A. dos Santos Fernandes

~ ~ ~

Win32-Specific

(CORE-1207) FB embedded would not load without extra OS privileges.

fixed by V. Khorsun

~ ~ ~

POSIX-Specific

(CORE-1240) Any task on Darwin PPC that used libfbclient would hang on exit.

fixed by A. Peshkov

~ ~ ~

(CORE-1223) Wrong message in firebird.log on Open SuSe Linux 10.2 : Open file limit increased from 1024 to 0.

fixed by V. Khorsun

~ ~ ~

Data Definition Language (DDL)

(CORE-1292) CREATE TABLE failed if using long username and UTF8 as attachment charset.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1271) Engine was allowing creation of invalid procedures and triggers.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1183) View could not be created if its WHERE clause contained IN <subquery> with a procedure reference.

fixed by D. Yemanov

~ ~ ~

(CORE-1162) Problem altering numeric field type.

fixed by C. Valderrama

~ ~ ~

Data Manipulation Language (DML)

(CORE-1253) LIST(DISTINCT) was concatenating VARCHAR values as CHAR

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1153) Activating an index change would cause “STARTING” to work as “LIKE” in a join condition.

fixed by A. dos Santos Fernandes

~ ~ ~

Procedural Language (PSQL)

(CORE-1267) Small bug with default value for domains in PSQL

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1256) Table columns were hiding the destination variables for RETURNING INTO.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1165) WHEN <list of exceptions> was tracking dependencies only on the first exception in PSQL.

fixed by C. Valderrama

~ ~ ~

Remote Interface

(CORE-1218) isc_dsql_info(isc_info_sql_stmt_type) did not set isc_info_end at the end of the passed user's buffer

fixed by V. Khorsun

~ ~ ~

(CORE-1196) Long SQL statements were breaking the TCP/IP connection.

fixed by V. Khorsun, A. Peshkov, D. Yemanov

~ ~ ~

Security

(CORE-885) It was impossible to revoke rights on update of a column.

fixed by A. Peshkov

~ ~ ~

(CORE-856) Could not set FName, MName, LName fields in the Security database to blank.

fixed by A. Peshkov

~ ~ ~

Utilities

nBackup

(CORE-1151) Error “database file not available” when running NBackup.

fixed by N. Samofatov

~ ~ ~

isql

(CORE-703) Using DEL-Key in isql under Linux would give “~”

fixed by A. Peshkov

~ ~ ~

gbak

(CORE-1237) gbak would fail to create a backup in service_mgr mode if there was no space on disk, but reported no error.

fixed by A. Peshkov

~ ~ ~

(CORE-1205) v2.1 gbak would crash the server when attempting to perform a backup.

fixed by D. Yemanov, C. Valderrama

~ ~ ~

(CORE-1174) gbak would restore NULL rdb$description in rdb$functions as blob (0, 0).

fixed by C. Valderrama

~ ~ ~

(CORE-949) Restore would fail with a UDF call in a 'COMPUTED BY' field.

fixed by D. Sibiryakov

~ ~ ~

(CORE-132) Restore would fail on external table.

fixed by V. Khorsun

~ ~ ~

gfix

(CORE-1249) Full shutdown mode failed on Classic if there were other connections to the database.

fixed by D. Yemanov

~ ~ ~

Building/Installers

(CORE-981) x86_64 RPM package missing “provides”.

fixed by A. Peshkov

~ ~ ~

(CORE-107) An instance of fb_lock_mgr would be left running after a build.

fixed by A. Peshkov

~ ~ ~

Fixed Regressions

(CORE-1286) Bug with COMPUTED BY fields.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1167) Character set GBK was not getting installed.

fixed by A. dos Santos Fernandes

~ ~ ~

Not Fixed

(CORE-1079) Every attach of fbclient/fbembed library to the host process leaks 64KB of memory

No information available.

~ ~ ~

Firebird 2.0 & Sub-Releases

Sub-release 2.0.5

Unregistered bug When Firebird is configured to run in some specific directory (/usr/local/firebird, /opt/firebird or any other) the @prefix@ macro should be substituted with that directory path. On MacOS it was not done and caused exceptions to be thrown when the engine tried to locate some of its components.

fixed by P. Beach

~ ~ ~

(CORE-2223) gbak was encountering several bugs when operating on the access control lists (ACLs) that store SQL privileges.

fixed by A. Peshkov

~ ~ ~

(CORE-2221) On POSIX platforms, any attachment to any database would fail after the access rights for security2.fdb were modified from 0660 to 0666.

fixed by P. Beach, A. Peshkov

~ ~ ~

(CORE-2108) When using the new implementation of Windows local protocol (XNET), the next available map number was calculated incorrectly, thus allowing the server to try to reuse a map number that already existed. If the “new” map's timestamp was equal to the timestamp of the pre-existing map, it was cause the `get_free_slot()` function to fail.

fixed by V. Horsun

~ ~ ~

(CORE-2078) The optimizer always had some trivial heuristics to estimate the effective stream selectivity, even if no indices could be used for the retrieval. This code missed being migrated into the ODS11 optimizer logic. The effect was that join orders chosen for cases involving non-indexed predicates were likely to be ineffective.

fixed by D. Yemanov

~ ~ ~

(CORE-2077) On POSIX platforms, the Classic server in embedded mode, i.e., loaded into the user's application space, would handle the TERM signal but would fail to call any other signal handlers in the queue. The effect was that signal handlers set by the application were not executed and the application would keep working after the termination. It was a bad idea to invoke `ISC_signal_cancel()` from the signal handler and the mechanism has been reworked.

fixed by A. Peshkov

~ ~ ~

(CORE-2073) The implementation of expression indexes exhibited a bug whereby an incorrect result was returned when an inverted Boolean predicate was applied to test an indexed expression.

fixed by D. Yemanov

~ ~ ~

(CORE-2065) The MacOSX installation package was in violation of platform rules by not including the client library in the dynamic loader search paths.

fixed by P. Beach

~ ~ ~

(CORE-2055) Backported a fix for a known buffer overflow in the Firebird client library.

fixed by A. Peshkov

~ ~ ~

(CORE-2050) Fixed a performance regression resulting from a surfeit of `semop()` system calls.

fixed by V. Horsun

~ ~ ~

(CORE-2049) Fixed a performance regression resulting from a surfeit of `sigprocmask()` system calls.

fixed by A. Peshkov

~ ~ ~

(CORE-2000) Under high load conditions, the lock manager could report false deadlocks.

fixed by V. Horsun

~ ~ ~

(CORE-1984) Lock manager would report false deadlocks if one of the deadlock participants was in WAIT with a permitted timeout.

fixed by V. Horsun

~ ~ ~

(CORE-1983) In any POSIX environment except Solaris, the engine was mishandling the “out of memory” condition, causing the server to crash.

fixed by A. Peshkov

~ ~ ~

(CORE-1982) Simultaneous backups or restores using the Services API under Superserver could interfere with one another.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1972) A non-SYSDBA user was able to change the Forced Writes mode of any database, along with several other database characteristics that should be restricted to the SYSDBA. This long-standing, legacy loophole in the handling of DPB parameters could lead to database corruptions or give ordinary users access to SYSDBA-only operations. The changes could affect several existing applications, database tools and connectivity layers (drivers, components). Details are in Chapter 3 of the accompanying Release Notes, in *Changes to the Firebird API and ODS*.

fixed by A. Peshkov

~ ~ ~

(CORE-1970) A “Lock conversion denied (bugcheck 215)” error could occur. This fix is related to CORE-1984 and CORE-2000 (above).

fixed by V. Horsun

~ ~ ~

(CORE-1958) When attempting to update the same record multiple times, a “Bugcheck 179 (decompression overran buffer)” failure could occur.

fixed by D. Yemanov

~ ~ ~

(CORE-1957) Because of a change done in the conversion to C++ at v.1.5, ACLs (Access Control Lists) longer than about 20 characters were being truncated. This has caused particular problems for applications that

construct access privileges in run-time and has also given rise to privileges “going missing” when there are more than about 2000 privileges (for a report of the latter, see Tracker issue CORE-216).

fixed by A. Peshkov

~ ~ ~

(CORE-1930) In a situation where a stored procedure was altered to remove output parameters and dependent procedures are not recompiled, the engine should properly track the dependencies and return an exception when the altered procedure is called. Instead, it was crashing.

fixed by V. Horsun

~ ~ ~

(CORE-1919) Memory corruptions in EXECUTE STATEMENT could crash the server.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1909) Garbage text was being printed to firebird.log on AMD64 Linux.

fixed by A. Peshkov

~ ~ ~

(CORE-1887) Newly created databases were being created on POSIX platforms with the wrong access rights. Now, access rights are set properly, by an explicit `chmod` call immediately after creation of the file.

fixed by A. Peshkov

~ ~ ~

(CORE-1886) On Windows Vista, the server would refuse to start as an application under a restricted user account.

This fix is a backport from the v.2.1 code that will need to be field-tested during RC.

fixed by N. Samofatov

~ ~ ~

(CORE-1884) Using expressions as the default values of input parameters for stored procedures could cause random server crashes.

fixed by V. Horsun

~ ~ ~

(CORE-1854) When using Unix native OS user authentication, the engine would return CURRENT_USER in the native (case-sensitive) form instead of the upper-cased form that Firebird user names should be resolved to.

fixed by A. Peshkov

~ ~ ~

(CORE-1844) Valgrind often reports “Conditional jump or move depends on uninitialised value(s)” in `check_status_vector()`, caused by poor data type matching which had the potential to corrupt the error status vector when there were multiple errors.

fixed by A. Peshkov

~ ~ ~

(CORE-1841) A view that used derived tables and long names for the tables or aliases could cause an overflow in RDB$VIEW_RELATIONS.RDB$CONTEXT_NAME.

fixed by V. Horsun

~ ~ ~

(CORE-1840) Every DDL request executed would leave a small memory leak.

fixed by D. Yemanov

~ ~ ~

(CORE-1830) Multiple updates of the same record in the same transaction, using savepoints, could corrupt indexes.

fixed by V. Horsun

~ ~ ~

(CORE-1826) The `changeRunUser.sh` and `restoreRootRunUser.sh` scripts on POSIX platforms were not changing the run user in the `init.d` scripts.

fixed by A. Peshkov

~ ~ ~

(CORE-1817) The `RelaxedAliasChecking` parameter was having no effect on RDB$DB_KEY.

fixed by V. Horsun

~ ~ ~

(CORE-1810) There were problems with user names containing the '.' character.

fixed by A. Peshkov

~ ~ ~

(CORE-1807) After an abnormal termination of Superserver on Linux, under a hard-to-reproduce situation where the “dead” `fbserver` process continued to listen on port 3050, the Guardian would retry port 3050 several times before giving up and assigning the new process to a non-canonical port. Meanwhile, client requests would go to port 3050 and hang indefinitely. Guardian needed to be restrained from such madness.

fixed by A. Peshkov

~ ~ ~

(CORE-1506) The server would crash with `isc_dsql_execute_immediate` and a zero-length string.

fixed by A. Peshkov

~ ~ ~

(CORE-1451) Using RDB$DB_KEY in a search argument when calling a selectable procedure would crash the server.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1439) Killing a Classic server process on a POSIX platform could corrupt databases.

fixed by A. Peshkov

~ ~ ~

(CORE-1357) The `DummyPacketInterval` mechanism was broken on all platforms.

fixed by D. Yemanov

~ ~ ~

(CORE-1313) Derived tables and the MERGE statement were failing to recognise RDB$DB_KEY.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1889) The security database was being created with Forced Writes off, risking corruption under some conditions.

fixed by A. Peshkov

~ ~ ~

Sub-release 2.0.4

(Unregistered nbackup Bugs) Bugs in nBackup could corrupt databases in some environments. The fixes relate to issues noted in heavy load conditions.

- The logic to merge the 'delta' file, which contains the pages which were changed since the nbackup was started, sometimes left the database in a corrupted state.
- The logic to merge the 'delta' file sometimes did not mark the database as “unlocked”, thus setting the database into an unreconcilable state.
- The logic to track which file to write the changed pages to had issues that could result in deadlocks when the backup/merge process was active.

fixed by N. Samofatov

~ ~ ~

(CORE-1820) The Windows installer would not correctly detect a running 2.0.x server if it was running without Guardian.

fixed by D. Yemanov, P. Reeves

~ ~ ~

(CORE-1775) Security checking during a prepare was performing badly.

fixed by V. Khorsun

~ ~ ~

(CORE-1774) The case-insensitive Spanish language collation ES_ES_CI_AI was exhibiting some problems.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1746) It was possible (but damaging) to create an expression index while inserts into the table were under way.

fixed by V. Khorsun

~ ~ ~

(CORE-1731) Under some conditions, the engine could “hang” for several minutes, using 100% of CPU resources without any input/output activity.

fixed by V. Khorsun

~ ~ ~

(CORE-1726) Failure could occur during `isc_service_start()`.

fixed by A. Peshkoff

~ ~ ~

(CORE-1702) Wrong record number calculation in garbage collector thread.

fixed by V. Khorsun

~ ~ ~

(CORE-1681) An incoming remote packet containing garbage data could crash the server.

fixed by D. Yemanov

~ ~ ~

(CORE-1680) The `gsec display` command was returning only the first few users from a security database that had more than 50 users installed in it.

fixed by A. Peshkoff

~ ~ ~

(CORE-1679) Output from `isc_service_query()` could contain garbage bytes.

fixed by A. Peshkoff

~ ~ ~

(CORE-1674) The /doc/ sub-directory on Linux installations was being installed without the appropriate access rights.

fixed by A. Peshkoff

~ ~ ~

(CORE-1657) Leaving a read-only, read-committed transaction idle for a long time could cause a memory access violation.

fixed by A. Peshkoff

~ ~ ~

(CORE-1644) Compilation error on GCC 4.1.1

fixed by A. Peshkoff

~ ~ ~

(CORE-1610) A Full server shutdown of Superserver would cause database corruption if it happened while a query modifying data was running.

fixed by D. Yemanov

~ ~ ~

(CORE-1603) A long user name had the potential to cause a buffer overflow.

A. Peshkoff

~ ~ ~

(CORE-1579) In the 64-bit builds, incorrect memory allocation for BLOB parameters in UDFs was causing the BLOB, if it was NULL and was followed by another parameter, to be overwritten by the value of the next parameter.

fixed by A. Peshkoff

~ ~ ~

(CORE-1572) The error “multiple rows in singleton select” was not being reported when it occurred in a view.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1549) Subquery-based predicates were are not being evaluated early enough in the join order.

fixed by D. Yemanov

~ ~ ~

(CORE-1533) A JOIN on an ordered derived table was returning the wrong first record.

fixed by D. Yemanov

~ ~ ~

(CORE-1501) `SLONG` data in `dsql_nod` was not being accessed correctly.

fixed by A. Peshkoff

~ ~ ~

(CORE-1500) Data in the internal buffer for `EXECUTE STATEMENT` was aligned incorrectly.

fixed by A. Peshkoff

~ ~ ~

(CORE-1434) Data used in INTL converters was aligned incorrectly.

fixed by A. Peshkoff

~ ~ ~

(CORE-1484) A memory access violation could occur in `fbintl`.

fixed by A. Peshkoff

~ ~ ~

(CORE-1481) GFIX could report false errors when using in-memory metadata.

fixed by V. Khorsun

~ ~ ~

(CORE-1476) Forced writes did not work on Linux at all.

fixed by A. Peshkov

~ ~ ~

(CORE-1470) With a multi-file database, the server would crash when a secondary file name exceeded 127 characters.

fixed by C. Valderrama

~ ~ ~

(CORE-1462) A buffer overrun would occur in the optimizer when more than 255 relation references existed in the query, causing the server to crash.

fixed by D. Yemanov

~ ~ ~

(CORE-1460) A client registering its interest in events would crash the server on being connected via the Named Pipes (WNet) protocol.

fixed by D. Yemanov

~ ~ ~

(CORE-1457) The server would crash on attempting to deliver events to a client session that had just disconnected.

fixed by V. Khorsun

~ ~ ~

(CORE-1456) Wrong events delivery was exhibited where there were multiple concurrent XNET connections.

fixed by V. Khorsun

~ ~ ~

(CORE-1455) An unsuccessful user management API call would cause the client library to crash.

fixed by A. Peshkoff

~ ~ ~

(CORE-1452) The client library would crash when attempting to process an event notification received just prior to disconnection.

fixed by D. Yemanov

~ ~ ~

(CORE-1447) A buffer overrun could occur when querying for database info through and `isc_database_info()` API call if the database path was very long.

fixed by C. Valderrama

~ ~ ~

(CORE-1434) The client library was misinterpreting the error condition created when isc_attach_database() was called to attach to a read-only database with a read-write transaction: it would return error code 0 instead of 335544727 (`net_write_err`).

fixed by D. Yemanov

~ ~ ~

(CORE-1421) SuperServer was unable to shut down immediately upon a shutdown request if a failed login attempt had preceded the request.

fixed by A. Peshkoff

~ ~ ~

(CORE-1419) CURRENT_TIMESTAMP evaluation was being performed incorrectly for selectable procedures.

fixed by D. Yemanov

~ ~ ~

(CORE-1199) Superserver could be brought down by an internal gds software consistency check (CCH_precedence: block marked (212), file: cch.cpp line: 3640).

fixed by V. Khorsun

~ ~ ~

(CORE-1194) An access violation could occur in the client library when a shutdown of Superserver was being handled.

fixed by D. Yemanov

~ ~ ~

(CORE-881) Singleton requirement was not being respected in COMPUTED BY expressions.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-100) An old bug in the Windows client library, dating back to v.1.5.3, could cause a memory access violation on disconnecting.

fixed by D. Yemanov

~ ~ ~

Sub-release 2.0.3

(CORE-1434) EXECUTE STATEMENT had suffered a regression between v.2.0.1 and v.2.0.2 whereby it was truncating VARCHAR variables.

This was the bug that caused Release 2.0.2 to be recalled. It was initially thought to have been caused by some anomaly related to the UTF-8 character set implementation but it was found to be a general fault affecting all varchars.)

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1418) Rapid starting and shutting down of multiple blocking AST threads was causing race conditions.

fixed by A. Peshkov

~ ~ ~

Sub-release 2.0.2

V.2.0.2 was withdrawn within hours of release because of the problems above.

(CORE-1405) A vulnerability would be manifest in attach/create database when the file name exceeded the MAX_PATH_LEN value.

fixed by A. Peshkov

~ ~ ~

(CORE-1403) In a situation where several events were being registered simultaneously by a client using an XNET connection, the server could crash.

fixed by D. Yemanov

~ ~ ~

(CORE-1400) GSTAT did not support the optional port number in the TCP/IP connection string.

fixed by D. Yemanov

~ ~ ~

(CORE-1399) GSTAT was not considering the RemoteServicePort option in firebird.conf

fixed by D. Yemanov

~ ~ ~

(CORE-1398) GSTAT was treating 'localhost' as case-sensitive on Windows.

fixed by D. Yemanov

~ ~ ~

(CORE-1397) Large network packets with garbage could result in big memory consumption and hign CPU load in a Superserver/TCP/IP environment, creating a vulnerability.

fixed by V. Khorsun

~ ~ ~

(CORE-1380) I/O errors would occur after changing the Forced Writes attribute of a database if there were other attachments to the databases.

fixed by V. Khorsun

~ ~ ~

(CORE-1371) An EXECUTE BLOCK statement within an EXECUTE STATEMENT string would fail.

fixed by A. Peshkov

~ ~ ~

(CORE-1349) The remote interface was failing to check (in REM_receive and REM_fetch calls) the length of client-supplied messages against the formatted length of the messages.

fixed by V. Khorsun

~ ~ ~

(CORE-1347) Certain conditions would cause unexpected “cannot transliterate” errors.

fixed by D. Yemanov

~ ~ ~

(CORE-1331) Character set transliterations were not working with EXECUTE STATEMENT.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1328) the gfix code for two-phase recovery operations with *gfix -t* was broken on POSIX, causing an unexpected end of input error.

fixed by A. Peshkov

~ ~ ~

(CORE-1312) A security vulnerability showed up, whereby a remote attacker could gain file access to a system running Firebird.

fixed by A. Peshkov

~ ~ ~

(CORE-1303) Superserver's remote listener could go into an infinite loop.

fixed by A. Peshkov

~ ~ ~

(CORE-1302) Some race conditions could occur during service startup.

fixed by A. Peshkov

~ ~ ~

(CORE-1300) Lower level index pages were being omitted from the parent page.

fixed by V. Khorsun

~ ~ ~

(CORE-1299) Wrong ordering of index entries was occurring at non-leaf b-tree pages.

fixed by V. Khorsun

~ ~ ~

(CORE-1298) The BTR\garbage_collect code could cause a deadlock in a page cache.

fixed by V. Khorsun

~ ~ ~

(CORE-1292) Attempting to create a table, when the connection had been made using a long user name and UTF8 as the attachment character set, would cause an exception.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1286) A bug with multi-byte characters was causing overflows and server crashes when a string value was applied to a COMPUTED BY field.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1279) Incorrect initialization of the engine would occur when many clients were attempting simultaneously to be the first to connect to Superserver.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1276) Sometimes, INET errors were being reported in firebird.log with an error code of 0 instead of the real error code.

fixed by V. Khorsun

~ ~ ~

(CORE-1265) Detaching from a database would deallocate the memory used by an active critical section.

fixed by D. Yemanov

~ ~ ~

(CORE-1249) Full shutdown mode would not work on Classic if there were other connections to the database.

fixed by D. Yemanov

~ ~ ~

(CORE-1248) Incorrect timestamp arithmetic would be performed when one of the operands was negative.

fixed by V. Khorsun

~ ~ ~

(CORE-1247) The BLOB garbage collection would remove the wrong BLOB if the departing BLOB's descriptor contained 0:0 ("Null value") but the field's NULL flag was not set.

fixed by V. Khorsun

~ ~ ~

(CORE-1240) With Darwin on PPC, any task using libfbclient, would hang on exit.

fixed by A. Peshkov

~ ~ ~

(CORE-1223) On openSUSE Linux 10.2 a nonsensical message could appear in firebird.log: “Open file limit increased from 1024 to 0”.

fixed by V. Khorsun

~ ~ ~

(CORE-1207) Since V. 2.0.1, all kernel objects created by the Firebird engine had their names prefixed with 'Global\' to cause them to be created in the global namespace and be accessible to processes running in different sessions. It also prevents possible database corruption.

On Windows 2003 and Vista, this requires SeCreateGlobalPrivilege, which is fine for a stand-alone server and clients. However, requiring for those extra privileges was no good for applications deployed with the embedded engine.

fixed by V. Khorsun

~ ~ ~

(CORE-1205) The v. 2.1 Beta gbak would crash the v2.0.x server when attempting to backup a database.

fixed by D. Yemanov, C. Valderrama

~ ~ ~

(CORE-1203) Some performance issues were encountered with certain queries on 32-bit Linux.

fixed by A. Peshkov

~ ~ ~

(CORE-1183) A view could not be created if its WHERE clause contained an IN <subquery> expression referring to a procedure.

fixed by D. Yemanov

~ ~ ~

(CORE-1156) PREPARE would fail when having an uncast parameter on the left side of a comparison with a subquery expression.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1153) STARTING [WITH] used for a join condition gave different results depending on whether a certain index was active or inactive.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1149) There was a vulnerability whereby the Services API could be used to effect a Denial-of-Service attack.

fixed by A. Peshkov

~ ~ ~

(CORE-1145) The server would lock up while attempting to commit the deletion of an expression index.

fixed by D. Yemanov

~ ~ ~

(CORE-1142) A generator's COMMENT could not be altered to the same value.

fixed by C. Valderrama

~ ~ ~

(CORE-984) On Windows, fbclient.dll would change the security descriptor of the calling process.

fixed by D. Yemanov, V. Khorsun

~ ~ ~

(CORE-968) A condition could occur that caused the client to lose its connection with the Firebird server.

fixed by A. Peshkov

~ ~ ~

(CORE-900) Attaching to a database simultaneously with the Services API and a standard API function could cause a deadlock.

fixed by A. Peshkov

~ ~ ~

Sub-release 2.0.1

(CORE-1140) The server would crash when performing garbage collection during index creation. The problem related to the existence of expression indices on the same table.

fixed by D. Yemanov

~ ~ ~

(CORE-1139) NBackup was failing to delete the delta file after a successful backup on Win32 Classic.

fixed by D. Yemanov

~ ~ ~

(CORE-1136) NBackup was not able to back up a recently created database.

fixed by D. Yemanov

~ ~ ~

(CORE-1133) The XNET (IPC) communication protocol would not work across session boundaries.

fixed by V. Khorsun

~ ~ ~

(CORE-1130) Bad optimization was occurring when a procedure was left joined with a view or subquery.

fixed by D. Yemanov

~ ~ ~

(CORE-1127) Circular index references in a corrupt database would cause fbserver to go into an infinite loop.

fixed by D. Downie, V. Khorsun

~ ~ ~

(CORE-1126) An arithmetic exception was being thrown when UNION sets involved UTF8 literals.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1124) NBackup would not work in interactive mode on Windows.

fixed by D. Yemanov

~ ~ ~

(CORE-1121) NBackup exhibited a page-level deadlock (bugcheck 215) when attempting to lock/back up a database under load.

fixed by D. Yemanov, G. Sergeev

~ ~ ~

(CORE-1110) The function isc_get_client_xxx_version() was not fully compatible with the InterBase version of the gds32.dll Windows client library.

fixed by V. Khorsun

~ ~ ~

(CORE-1104) The Linux install would fail if the x0rfbserver program was running.

fixed by A. Peshkov

~ ~ ~

(CORE-1025) The server would crash at runtime when an explicit MERGE plan was specified over multiple JOIN elements.

fixed by D. Yemanov

~ ~ ~

(CORE-1016) Checking the configured UdfAccess setting was not being performed until after the library had been loaded and its startup code had been executed.

fixed by A. Peshkov

~ ~ ~

(CORE-943) Database shutdown was being executed incorrectly when the database was in physical backup mode.

fixed by D. Yemanov

~ ~ ~

(CORE-1094) isc_dsql_sql_info() was returning unordered SQLVAR descriptors

fixed by D. Yemanov

~ ~ ~

(CORE-1080) Bugcheck 167 (invalid SEND request) occurring in Superserver

This was a long-standing bug in Superserver: when several parallel attachments began executing a trigger that had not yet been loaded into the metadata cache, the first of them would compile the trigger request's BLR but others would not wait until the request compilation finished. Hence, other attachments would execute a NULL request.

Protection from such failures existed in MET_procedure using dbb_sp_rec_mutex for stored procedures, but not for triggers.

fixed by V. Khorsun

~ ~ ~

(CORE-1012) Since Firebird 1.5.3, neither the relation name nor the alias was being returned for columns participating in a GROUP BY aggregation with joins.

This problem was reported to affect particularly applications using IB Objects, which maintains internal structures to support “live” searching of tables underlying joined and aggregated sets.

fixed by A. Dos Santos Fernandes

~ ~ ~

(CORE-1068) isql was not printing non- nullable blobs, due to incorrect checking of the XSQLVAR structure.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1064) The backup order in gbak was wrong for character sets and collations.

Character sets and collations were being backed up after tables and hence they were being restored after tables. The problem became obvious when restoring with the -ONE_AT_A_TIME switch, where a table definition used non-system character sets or collations.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1063) The Server could hang, eating CPU and performing huge I/O copying different codepage fields.

Under certain conditions, notably when multi-byte character sets were involved, an endless loop or a transliteration exception could occur wherein BLOB segments of zero length were being created and empty BLOB pages were being stored until resources were exhausted.

fixed by V. Khorsun

~ ~ ~

(CORE-944, CORE-982, CORE-1059) This set of bug fixes fixed cases reported in several crash reports on POSIX platforms, involving execution of stored procedures where both BLOBs and external function calls were involved.

fixed A. Peshkov

~ ~ ~

(CORE-1057) GSEC was exhibiting a bug where it was hiding errors on a call to CryptAcquireContext().

fixed by A. Peshkov, A. dos Santos Fernandes

~ ~ ~

(CORE-1055) Parameter matching for self-referencing stored procedures was wrong.

fixed by D. Yemanov

~ ~ ~

(CORE-1053) A SELECT statement could return invalid results when an index was to evaluate a “greater than” predicate in a WHERE clause. The erroneous logic would occur if the key value changed exactly at the beginning of the index block.

For example, the statement

```
SELECT * FROM Table WHERE IntField > Constant
```

would return fewer records than

```
SELECT * FROM Table WHERE IntField >= Constant+1
```

fixed by A. Peshkov, A. Brinkman

~ ~ ~

(CORE-1051) A bug was found in DFW\check_dependencies that could corrupt the stack.

fixed by V. Khorsun

~ ~ ~

(CORE-1046) A bug was causing a core dump in CVT_move.

fixed by D. Yemanov

~ ~ ~

(CORE-1040) A wrong single-segment ascending index could occur on a character field if there were NULLs and empty string values in the column.

fixed by V. Khorsun, A. Brinkman

~ ~ ~

(CORE-1020, CORE-1037) Some inconsistencies of installation components could happen with command-line use of the Win32 Installer. The problem areas were fixed.

> **Note**
>
> Previously, the Guardian was installed by default, whether the Classic or Superserver installation was selected. In Firebird 2.0 and higher, Guardian is not installed with Classic and should not be. It is not necessary and, in some Classic environments, it has been considered a possible cause of “ghost connections” and, thus, resource leakage.

fixed by P. Reeves

~ ~ ~

(CORE-1033) In some views, the LIKE clause would not work for computed values.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-1029) Bad plans could be generated for queries with outer joins having IS NULL clauses, depending on the order of the search predicates.

fixed by D. Yemanov

~ ~ ~

(CORE-1020) The server could crash at run-time when an explicit MERGE plan was specified to override one that would have used a few JOIN phrases instead.

fixed by D. Yemanov

~ ~ ~

(CORE-1017) Windows service attachments using the Xnet protocol would fail when Classic had been started with the -x -i (Xnet and TCP/IP) parameters set.

fixed by D. Yemanov

~ ~ ~

(CORE-1011) The server would crash if an application tried to connect to it via an InterBase version of gds32.dll.

fixed by A. Peshkov, D. Yemanov

~ ~ ~

(CORE-1010) The server could crash if an executing DDL statement raised an exception.

fixed by D. Yemanov

~ ~ ~

(CORE-1006) Rollback or garbage collection would cause an access violation (segfault) if an updated table had an expression index defined by a subquery.

fixed by V. Khorsun

~ ~ ~

(CORE-1005) A DISTINCT query that specifed NULLS LAST in an ORDER BY clause would return NULLs in the wrong position.

fixed by D. Yemanov

~ ~ ~

(CORE-1004) Conditions could occur where the error “Context already in use (BLR error)” would be wrongly thrown when accessing explicit cursors in PSQL.

fixed by D. Yemanov

~ ~ ~

(CORE-997) An old bug with indices on a character column with a COLLATE attribute became more visible and made it impossible to upgrade the database from ODS 10.1 to ODS 11. The restore would wrongly report the error “internal gds software consistency check (index key too big (nnn))”.

fixed by A. dos Santos Fernandes

~ ~ ~

(CORE-988) On Linux, using the 32-bit Superserver with the old threading model, the server would repeatedly crash.

Due to a bug in some versions of glibc, errno contained garbage after sem_timedwait(). Obviously, a clean fix is not in order. However, considering that people often try to use Firebird with such buggy versions and tend to blame Firebird for the problem, and that upgrading glibc is not trivial operation for many, a hack has been done to the body of the class semaphore. It now works correctly with both the normal and the broken versions of glibc.

fixed by A. Peshkov

~ ~ ~

(CORE-984) Using the Windows client (fbclient.dll) to open a database connection was changing the security descriptor of the process that called the library functions, making it impossible for other processes to share handles with synchonization objects or with other handles.

fixed by D. Yemanov

~ ~ ~

(CORE-966) Socket binding for events exhibited bugs whereby the *setsockopt* call in inet.cpp was using an uninitialised variable and did not handle errors properly. It resulted in "INET/inet_error: bind errno = 10048" errors reported in the log whenever clients bound to database events.

fixed by P. Beach

~ ~ ~

(CORE-959) gstat would not work using the localhost connection string.

Since v1.5, it has been possible to run gstat using a pseudo-remote connection string (localhost:<path>) but it was broken in v2.0.

fixed by D. Yemanov

~ ~ ~

(CORE-952) Using a BLOB in an expression index would cause an access violation (segfault).

fixed by V. Khorsun

~ ~ ~

(CORE-888) A number of people reported getting the "Object in use" when attempting to alter, recreate, replace or drop a stored procedure or trigger whilst the existing trigger or SP was in use. It was not a bug, per se, but an intentional restriction.

The restriction has been removed (reverted to 1.5 behaviour). Thus it is again possible to perform these types of DDL operations on "live" objects, and incur the same "window of unpredictable effect" for Classic users as in previous versions.

Reversion done by D. Yemanov

~ ~ ~

Firebird 2.0

The following bugs present in Firebird 1.5 were fixed in v.2.0. Note that, in many cases, the bug-fixes were backported to Firebird 1.5.x sub-releases.

General Engine Bugs

(CORE-911) Leaving a Classic server process idle for a long period while a read-only, Read Committed transaction was active could cause segmentation faults/AVs.

fixed by V. Khorsun

~ ~ ~

(CORE-902) The server could crash intermittently during execution of DDL or DML statements.

fixed by V. Khorsun

~ ~ ~

Not registered Assignments to columns deleted by a concurrent transaction were being improperly allowed.

fixed by D. Yemanov

~ ~ ~

Not registered Error "invalid transaction handle" would be thrown when calling isc_array_lookup_bounds() from multiple threads.

fixed by D. Yemanov

~ ~ ~

Not registered Heavy concurrent load could cause index data corruption.

fixed by V. Khorsun

~ ~ ~

SF #1446987 BLOBs could appear to be damaged during operations in PSQL, causing a "BLOB not found" error.

fixed by V. Khorsun

~ ~ ~

SF #1434147 Bugs with COUNT (DISTINCT XXXX) when XXXX was a high integer.

fixed by V. Khorsun

~ ~ ~

SF #1435997 A bug was causing a close database error -901 on the embedded server.

fixed by D. Yemanov

~ ~ ~

SF #1436066 Adding an index during database activity could cause logical errors in structure that GFIX would detect.

fixed by V. Khorsun

~ ~ ~

Not registered A few types of subqueries were being wrongly treated as variant, causing performance issues.

fixed by D. Yemanov

~ ~ ~

Not registered Previously, the Transaction ID would silently (and dangerously) overflow. Now it will throw a consistency check when it reaches the limit (which is still 2^31).

fixed by V. Khorsun

~ ~ ~

Not registered Read committed transactions would block garbage collection unnecessarily.

fixed by V. Khorsun

~ ~ ~

Not registered The ALL predicate could return wrong results.

fixed by D. Yemanov

~ ~ ~

SF #1404157 DFW was not ready for RECREATE TABLE/VIEW

fixed by D. Yemanov

~ ~ ~

Not registered Restored the code which replaces ROLLBACK with COMMIT if a transaction has not modified any data.

fixed by D. Yemanov

~ ~ ~

Not registered There were some bugs producing wrong statistics:

- with relation/index data longer than 2^32 bytes
- when the average index key length rounded to an integer value

fixed by V. Khorsun

~ ~ ~

Not registered Attaching with the isc_dpb_no_garbage_collect option was forcing a sweep.

fixed by V. Khorsun

~ ~ ~

Not registered The system transaction was being reported as dead.

fixed by A. dos Santos Fernandes, V. Khorsun

~ ~ ~

Not registered The server would lock up after an unsuccessful attach to the security database.

fixed by D. Yemanov, C. Valderrama

~ ~ ~

SF #1076858 Source of possible corruption in Classic server.

fixed by V. Khorsun

~ ~ ~

SF #1116809 Incorrect data type conversion.

fixed by A. dos Santos Fernandes

~ ~ ~

SF #1111570 Problem dropping a table having a check constraint referencing more than one column.

fixed by C. Valderrama

~ ~ ~

Not registered Usage of an invalid index in an explicit plan caused garbage to be shown in the error message instead of the rejected index name.

fixed by C. Valderrama

~ ~ ~

SF #543106 Bug with ALL keyword. MORE INFO REQUIRED.

fixed by D. Yemanov

~ ~ ~

Not registered System users "AUTHENTICATOR" and "SWEEPER" were lost, causing "SQL SERVER" to be reported instead.

fixed by A. Peshkov

~ ~ ~

Not registered Don't rollback prepared 2PC sub-transaction. (Description needs clarifying, Vlad!)

fixed by V. Khorsun

~ ~ ~

Not registered Memory consumption became exorbitant when blobs were converted from strings during request processing. For example, the problem would appear when running a script with a series of statements like

```
insert into t(a,b)
   values(N, <literal_string>);
```

when b was blob and the engine was performing the conversion internally.

fixed by N. Samofatov

~ ~ ~

Not registered Materialization of BLOBs was not invalidating temporary BLOB IDs soon enough.

A blob is created as an orphan. This blob has a blob id of {0,slot}. It is volatile, meaning that, if the connection terminates, it will become eligible for garbage collection. Once a blob is assigned to field in a table, it is said to be materialized. If the transaction that did the assignment commits, the blob has an anchor in the table and will be considered permanent. Its blob id is {relation_id,slot}.

In situations where internal code is referencing the blob by its old, volatile blob id, the references are "routed" to the materialized blob, until the session is closed.

fixed by N. Samofatov

Solution Now, the references to a volatile blob are checked and, when there are no more references to it, it is invalidated.

~ ~ ~

Not registered Conversion from string to blob had a memory leak.

fixed by N. Samofatov

~ ~ ~

SF #750664 Issues with read-only databases and transactions.

fixed by N. Samofatov

~ ~ ~

Not registered When one classic process dropped a foreign key and another process was trying to delete master record, the error 'partner index not found' would be thrown.

fixed by V. Khorsun

~ ~ ~

Various server bugs

1. eliminated redundant attempts to get an exclusive database lock during shutdown
2. corrected inaccurate timeout counting
3. database lock was not being released after bringing database online in the exclusive mode
4. removed a 5 sec timeout when bringing database online in the shared mode

fixed by D. Yemanov

~ ~ ~

SF #1186607 Foreign key relation VARCHAR <-> INT should not have caused an exception.

fixed by V. Khorsun

~ ~ ~

SF #1211325 Fixed problems with BLOBs in external tables.

fixed by V. Khorsun

~ ~ ~

Not registered After an attempt to "create view v(c1) as select 1 from v" all clones of the system request would remain active forever.

fixed by A. Peshkov

~ ~ ~

SF #1191006 Use of WHERE params in SUM would return incorrect results.

fixed by A. Brinkman

~ ~ ~

SF #750662 Fixed a bug involving multiple declaration of blob filters.

fixed by D. Yemanov

~ ~ ~

SF #743679 FIRST / SKIP was not as well implemented as it could be.

fixed by D. Yemanov

~ ~ ~

Not registered CPU load would rise to 100% when an I/O error caused a rollover to a non-existent shadow.

fixed by D. Yemanov

~ ~ ~

Not registered "Cannot find record fragment" bugcheck could occur during garbage collection on the system tables.

fixed by V. Khorsun

~ ~ ~

SF #1211328 Error reporting cited maximum BLOB size wrongly.

fixed by D. Yemanov

~ ~ ~

SF #1292007 Duplicated field names in INSERT and UPDATE statements were getting through.

fixed by C. Valderrama

~ ~ ~

Not registered The SQL string was being stored truncated within the RDB$*_SOURCE columns in some cases

fixed by D. Yemanov

~ ~ ~

Not registered Broken implementation of the MATCHES predicate in GDML

fixed by D. Yemanov

~ ~ ~

SF bug #1404215 Column dependencies were not being stored for views.

fixed by D. Yemanov

~ ~ ~

SF bug #1191206 A few constraint issues.

fixed by D. Yemanov

~ ~ ~

SF bug #609538 Alter Index on a Foreign Key index should cause an exception and it did, but the error message was not appropriate.

fixed by D. Yemanov

~ ~ ~

SF bug #1175157 An error in the thread scheduler was causing the server to lock up.

fixed by V. Khorsun

~ ~ ~

Not registered

1. Improper thread data operations were occurring during the protocol port cleanup
2. Transaction rollback and attachment cleanup for broken TCP connections was faulty

fixed by V. Khorsun, D. Yemanov

~ ~ ~

Not registered A wrong error message was decoded when firebird.msg was missing or outdated.

fixed by D. Yemanov

~ ~ ~

Not registered Buffer overflows inside the BLR->ASCII blob filter were causing memory corruption and server crashes.

fixed by D. Yemanov

~ ~ ~

Not registered A successful status vector could be reported to the user after a failed DDL operation.

fixed by V. Khorsun

~ ~ ~

Not registered Threading issues in the DSQL metadata cache were causing unexpected “invalid transaction handle” errors under load.

fixed by D. Yemanov

~ ~ ~

Not registered Wrong results would be returned by the division operation after DDL changes.

Example

```
create table test(fld numeric(18, 2));
insert into test (fld) values (1);
commit;
alter table test alter fld type numeric(18,3);
select fld/3 from test; -- returns 0.033 instead of expected 0.333
```

fixed by D. Yemanov

~ ~ ~

SF #1184099 Incorrect padding was exhibited when using character set OCTETS.

fixed by C. Valderrama, A. dos Santos Fernandes

~ ~ ~

Not registered Unexpected errors were occurring because of improperly handled dead record versions created by the system transaction during DDL operations.

fixed by A. Harrison

~ ~ ~

SF #223060 Processing of the GREATER-THAN operator was too slow.

fixed by V. Khorsun

~ ~ ~

Not registered CHECK constraints were not SQL-compliant with regard to the handling of NULL. Until now, if NULL were to be allowed, it had to be specified explicitly in the constraint definition. Under the standard, NULL is allowed unless explicitly constrained by NOT NULL or CHECK (.. IS NOT NULL).

Example of Problem

The following definition now allows NULL in DEPTNO, where previously it did not:

```
CHECK (DEPTNO IN (10, 20, 30))
```

fixed by P. Ruizendaal, D. Yemanov

~ ~ ~

Not registered It was possible to create a primary key constraint on a column consisting of NULLs.

Example of Problem

```
create table bug (f1 int not null, f2 int not null);
insert into bug (f1, f2) values (1, 1);
commit;
alter table bug add pk int not null primary key;
```

fixed by V. Khorsun

~ ~ ~

SF #1334034 REVOKE was damaging the ACL (Access Control List).

fixed by D. Yemanov

~ ~ ~

Services Manager

Not registered Incorrect encryption of password when the Services Manager was invoked by the Embedded client.

fixed by A. Peshkov

~ ~ ~

GFix Bugs

SF #1242106 Shutdown bugs:

1. Incorrect commit instead of rollback during shutdown
2. Crash or bugcheck during SuperServer shutdown with active attachments

fixed by D. Yemanov

~ ~ ~

Not registered Crash occurred in service gfix code when it tried to reattach to a currently unavailable database. Since a service cannot interact with the end-user, an endless loop leads to overflowing the service buffer and causing a crash as a result.

fixed by V. Khorsun

~ ~ ~

DSQL Bugs

SF #1408079 The parser was not validating string literal markers.

fixed by C. Valderrama

~ ~ ~

Not registered The engine would fail to parse the SQL ROLE keyword properly.

fixed by C. Valderrama

~ ~ ~

Not registered EXECUTE PROCEDURE did not check SQL permissions at the prepare stage.

fixed by D. Yemanov

~ ~ ~

SF #217042 Weird SQL constructions are not always properly validated.

Partly fixed by C. Valderrama

~ ~ ~

SF #1108909 View could be created without rights on a table name like "a b"

fixed by C. Valderrama

~ ~ ~

SF #512975 Clear embedded spaces and CR+LF before DEFAULT clauses when storing them in system tables

Implemented by C. Valderrama

~ ~ ~

SF #910423 Anomaly with ALTER TABLE altering a column's type to VARCHAR, when determining valid length of the string.

```
SQL> CREATE TABLE tab ( i INTEGER );
SQL> INSERT INTO tab VALUES (2000000000);
SQL> COMMIT;

SQL> ALTER TABLE tab ALTER i TYPE VARCHAR(5);
Statement failed, SQLCODE = -607
unsuccessful metadata update
-New size specified for column I must be at least 11 characters.
```

i.e., it would need potentially 10 characters for the numerals and one for the negative sign.

```
SQL> ALTER TABLE tab ALTER i TYPE VARCHAR(9);
```

This command should fail with the same error, but it did not, which could later lead to unreadable data:

```
SQL> SELECT * FROM tab;
I
=========
Statement failed, SQLCODE = -413
conversion error from string "2000000000"
```

fixed by C. Valderrama

~ ~ ~

Not registered There were some rounding problems in date/time arithmetic.

fixed by N. Samofatov

~ ~ ~

Not registered Line numbers in DSQL parser were being miscounted when multi-line literals and identifiers were used.

fixed by N. Samofatov

~ ~ ~

SF #784121 Some expressions in outer join conditions were causing problems.

fixed by C. Valderrama

~ ~ ~

Not registered There were some dialect- specific arithmetic bugs:

Dialect 1

1. '1.5' / '0.5' did not work
2. avg ('1.5') did not work
3. 5 * '1.5' produced an INT result instead of DOUBLE PRECISION
4. sum ('1.5') produced a NUMERIC(15, 2) result instead of DOUBLE PRECISION
5. - '1.5' did not work

Dialect 3

- '1.5' * '0.5' and '1.5' / '0.5' were not forbidden, but they should have been.

fixed by D. Yemanov

~ ~ ~

SF #1250150 There was a situation where a procedure could not be dropped.

fixed by V. Khorsun

~ ~ ~

SF #1238104 Internal sweep report was incorrect.

fixed by C. Valderrama

~ ~ ~

SF #1371274 The infamous “Datatype unknown” error when attempting some castings has been eliminated. It is now possible to use CAST to advise the engine about the data type of a parameter.

fixed by D. Yemanov

~ ~ ~

SF #1292106 ORDER BY with FOR UPDATE WITH LOCK would trash the index.

fixed by D. Yemanov

~ ~ ~

SF #1368741 UPPER() was returning wrong results.

fixed by A. dos Santos Fernandes

~ ~ ~

PSQL Bugs

(CORE-921) A bug in EXECUTE STATEMENT implementation could cause a core dump during PSQL execution.

fixed by A. Peshkov

~ ~ ~

SF #1422471 A memory leak was exhibited in EXECUTE STATEMENT.

fixed by A. Peshkov

~ ~ ~

Not registered ROW_COUNT was getting cleared after SUSPEND execution.

fixed by D. Yemanov

~ ~ ~

SF #1124720 Problem with "FOR EXECUTE STATEMENT ... DO SUSPEND;"

fixed by A. Peshkov

~ ~ ~

Not registered Memory leakage was occurring when selectable stored procedures were called from PSQL or in subqueries.

fixed by N. Samofatov

~ ~ ~

Not registered The wrong error would be reported when non-active contexts were accessed in multi-action triggers.

fixed by D. Yemanov

~ ~ ~

Not registered An internal error was reported when attempting to pass/return blobs to/from string functions inside PSQL.

fixed by D. Yemanov

~ ~ ~

Crash Conditions

Not registered A crash could occur if some bad client passed more than the supported number of remote protocol versions.

fixed by A. Karyakin, A. Peshkov

~ ~ ~

Not registered An AV could occur when the server was configured to use TCP packets as large as 32 Kb.

fixed by C. Valderrama, A. Peshkov

~ ~ ~

Not registered Server would crash if a positioned UPDATE/DELETE executed via DSQL was referencing a cursor that had already been released.

fixed by V. Khorsun

~ ~ ~

Not registered Certain DDL actions could crash the server.

Example of a problem action

```
alter table rdb$relations
  add rdb$garbage varchar(30);
```

fixed by J. Starkey

~ ~ ~

Not registered An overflow in the plan buffer would cause the server to crash.

fixed by D. Yemanov

~ ~ ~

Not registered Possible server lockup/crash when 'RELEASE SAVEPOINT xxx ONLY' syntax is used or when existing savepoint name is reused in transaction context

fixed by N. Samofatov

~ ~ ~

Not registered Rare client crashes caused by improperly cleaned XDR packets.

fixed by D. Yemanov

~ ~ ~

Not registered Server crash during SuperServer shutdown

fixed by A. Peshkov

~ ~ ~

SF #1057538 The server would crash if the output parameter of a UDF was not the last parameter.

fixed by C. Valderrama

~ ~ ~

Not registered A number of possible server crash conditions had been reported by Valgrind.

fixed by N. Samofatov

~ ~ ~

Not registered Server would crash when a wrong type or domain name was specified when changing the data type for a column.

fixed by N. Samofatov

~ ~ ~

Not registered Incorrect accounting of attachment pointers used inside the lock structure was causing the server to crash.

fixed by N. Samofatov

~ ~ ~

Not registered In v.1.5, random crashes would occur during a restore.

fixed by J. Starkey

~ ~ ~

Not registered Crash/lock-up with multiple calls of isc_dsql_prepare for a single statement.

fixed by N. Samofatov

~ ~ ~

Not registered Server would crash when the system year was set too high or too low.

fixed by D. Yemanov

~ ~ ~

Not registered Server would crash when the stream number exceeded the limit.

fixed by D. Yemanov

~ ~ ~

Not registered Server would crash when outer aggregation was performed and explicit plans were used in subqueries.

fixed by D. Yemanov

~ ~ ~

Not registered DECLARE FILTER would cause the server to crash.

fixed by A. Peshkov

~ ~ ~

Not registered The server would crash when a PLAN for a VIEW was specified but no table alias was given.

fixed by V. Khorsun

~ ~ ~

Not registered Server would crash during the table metadata scan in some cases.

fixed by D. Yemanov

~ ~ ~

Not registered Server would crash when too big a key was specified for an index retrieval.

fixed by D. Yemanov

~ ~ ~

Not registered Server would crash when manipulating input DPB due to memory corruption in Parameter Blocks management.

fixed by C. Valderrama

~ ~ ~

Not registered Server would crash when attempting to restore a database backup with corrupted VARCHAR data.

fixed by D. Yemanov

~ ~ ~

Remote Interface Bugs

Not registered A TCP/IP buffer size larger than 32 Kb was not being processed correctly.

fixed by A. Peshkov

~ ~ ~

Not registered The NO_NAGLE option was working improperly.

fixed by F. Polizo, A. Peshkov

~ ~ ~

Not registered NO_NAGLE and KEEPALIVE socket options were not enabled for CS builds.

fixed by D. Yemanov

~ ~ ~

SF #1385092 A TCP/IP connection would appear to freeze the Superserver if it was disconnected abnormally while a large packet, e.g. a BLOB or a large SQL request, was being passed across the interface.

This was a long-standing InterBase/Firebird bug in the implementation of the protocol layer for Superserver on Windows. Borland invented two different thread management strategies: one for TCP/IP and one for the other protocols that only Windows supports, i.e. Named Pipes (sometimes referred to as “NetBEUI”) and the IPServer local connection. This bug occurred only with TCP/IP connections.

For TCP/IP, a multiplexing loop (main server loop), which is common for all ports, receives API packets from clients, creates requests and sends them to threads for processing. When it detects an incoming packet, it starts to receive it from the port.

Before this fix, it needed the entire API packet to come at once. However, in the course of converting a packet to a request (done by the XDR protocol), in cases where the size of the API packet happened to be greater than that of the network packet, the server had to wait for the next network packet from the port.

At this point, ports were being scanned for incoming packets only by calculating (timeout - interval since last packet received) for each port in the loop. If the next packet from a particular port did not come, for example because of an unplugged jack, the only way to interrupt this receive and allow the main server loop to carry on processing the other ports was to wait for the keepalive TCP timeout to elapse on the abandoned connection. Given that the default keepalive value is two hours, it would appear that the Superserver was “hung”.

fixed by A. Peshkov

~ ~ ~

SF #1260310 Nessus vulnerability scanning could cause the server to drop connections.

fixed by A. Peshkov

~ ~ ~

SF #1065511 Clients on Windows XP SP2 were slow connecting to a Linux server.

fixed by N. Samofatov

~ ~ ~

SF #1065511 Clients on Windows XP SP2 were slow connecting to a Linux server.

fixed by N. Samofatov

~ ~ ~

SF #571026 INET/INET_connect: gethostbyname was not working properly.

fixed by D. Yemanov

~ ~ ~

SF #223058 Multi-hop server capability was broken.

fixed by D. Yemanov

~ ~ ~

Not registered Fixed memory leak from connection pool in isc_database_info.

fixed by N. Samofatov

~ ~ ~

Not registered Database aliases were not working in WNET.

fixed by D. Yemanov

~ ~ ~

Not registered Client would crash while disconnecting with an active event listener.

fixed by D. Yemanov

~ ~ ~

Not registered The client library would not react to environment variables being set via SetEnvironment-Variable().

fixed by C. Valderrama

~ ~ ~

Indexing & Optimization

SF #459059D Index breaks = ANY result. MORE INFO REQUIRED.

fixed by N. Samofatov

~ ~ ~

Not registered Ambiguous queries were still possible under some conditions.

fixed by A. Brinkman

~ ~ ~

SF #735720 SELECT ... STARTING WITH :v was wrong when :v = ''

fixed by A. Brinkman

~ ~ ~

Not registered There were issues with negative dates, i.e. those below Julian date [zero], when stored in indices.

fixed by A. Brinkman

~ ~ ~

SF #1211354 Redundant evaluations were occurring in COALESCE.

fixed by A. Brinkman

~ ~ ~

Not registered Error "index key too big" would occur when creating a descending index.

fixed by V. Khorsun

~ ~ ~

SF #1242982 Bug in compound index key mangling.

fixed by A. Brinkman

~ ~ ~

Vulnerabilities

SF #1466193 Semaphore array`s permissions in fb_lock_mgr were 0666 - i.e., anyone could lock them and block all subsequent queries.

fixed by A. Peshkov

~ ~ ~

Not registered Possible buffer overflow in WNET.

fixed by A. Peshkov

~ ~ ~

Not registered Several buffer overflows were fixed.

fixed by A. Peshkov

~ ~ ~

SF #1155520 Fixed a vulnerability that could make it possible for a user who was neither SYSDBA nor owner to create a database that would overwrite an existing database.

fixed by A. dos Santos Fernandes

~ ~ ~

ISQL Bugs

SF #781610 Comments in ISQL using '--' were causing problems.

fixed by J. Bellardo, B. Rodriguez Samoza

~ ~ ~

Not registered ISQL_disconnect_database was overwriting the Quiet flag permanently.

fixed by M. Penchev, C. Valderrama

~ ~ ~

SF #1208932 SHOW GRANT did not distinguish object types.

fixed by C. Valderrama

~ ~ ~

SF #494981 Bad exception report.

fixed by C. Valderrama

~ ~ ~

SF #450404 ISQL would uppercase role in the command line.

fixed by C. Valderrama

~ ~ ~

Various, not registered

1. Fix for the -b (Bail On Error) option when SQL commands are issued and no db connection exists yet.
2. Applied Miroslav Penchev's patch for bug with -Q always returning 1 to the operating system, discovered by Ivan Prenosil.

fixed by M. Penchev, C. Valderrama

~ ~ ~

Not registered Metadata extraction for triggers, check constraints and views with check option was wrong.

fixed by C. Valderrama, D. Yemanov

~ ~ ~

International Character Set Bugs

SF #1016040 Missing external libraries would cause an engine exception.

fixed by A. dos Santos Fernandes

~ ~ ~

Not registered

1. Charset/collation issues for expression-based view columns
2. Lost charset/collation for local PSQL variables

fixed by D. Yemanov

~ ~ ~

Not registered Comparisons between strings in NONE and another character set would cause an error.

fixed by D. Yemanov, A. dos Santos Fernandes

~ ~ ~

SF #1244126 There was a problem updating some text BLOBs when connected with character set NONE.

fixed by A. dos Santos Fernandes

~ ~ ~

SF #1242379 Applying a collation could change a VARCHAR's length

fixed by A. dos Santos Fernandes

~ ~ ~

SQL Privileges

Not registered Permissions were not being checked for view columns.

fixed by D. Yemanov

~ ~ ~

Not registered Privileges granted to procedures/triggers/views were being preserved after the object had been dropped.

fixed by D. Yemanov

~ ~ ~

Not registered Column-level SQL privileges were being preserved after the affected column was dropped.

fixed by D. Yemanov

~ ~ ~

SF #223128 SYSDBA could grant non-existent roles

fixed by D. Yemanov

~ ~ ~

UDF Bugs

Not registered There were thread safety issues in datetime functions of the FBUDF library.

fixed by C. Valderrama

~ ~ ~

Not registered The UDF AddMonth() in the UDF library FBUDF had a bug that displayed itself when the calculation rolled the month past the end of the year.

fixed by C. Valderrama

~ ~ ~

Not registered Diagnostics when a UDF module was missing/unusable needed improvement.

fixed by A. Peshkov

~ ~ ~

Not registered There were some problems with the mapping of UDF arguments to parameters.

fixed by N. Samofatov

~ ~ ~

Not registered UDF arguments were being prepared/optimized twice.

fixed by D. Yemanov

~ ~ ~

SF #544132, #728839 Nulls handling in UDFs was causing problems.

fixed by C. Valderrama

~ ~ ~

Not registered UDF access checking was incorrect.

fixed by D. Yemanov

~ ~ ~

gbak

Not registered There were issues with restoring if indexes used in explicit plans inside PSQL code had been dropped.

fixed by A. dos Santos Fernandes

~ ~ ~

Not registered *gbak* could not restore a database containing broken foreign keys.

Now, the restore continues to run, the user gets a diagnostic indicating which FK caused the problem. The affected index becomes inactive and, after restore, the database is left in shutdown state.

fixed by A. Peshkov

~ ~ ~

Not registered *gbak* would stall when used via the Services Manager and an invalid command line was passed.

fixed by V. Khorsun

~ ~ ~

Not registered A computed column of a blob or array type would zero values in the first column of the table being restored.

fixed by D. Yemanov

~ ~ ~

Not registered Fixed some backup issues with stream BLOBs that caused them to be truncated under some conditions.

fixed by N. Samofatov

~ ~ ~

Not registered Interdependent views caused problems during the restore process.

fixed by A. Brinkman

~ ~ ~

SF #750659 If you want to start a fresh db, you should be able to restore a backup done with the metadata-only option. Generator values were resisting metadata-only backup and retaining latest values from the live database, instead of resetting the generators to zero.

fixed by C. Valderrama, D. Yemanov

~ ~ ~

SF #908319 In v.1.5, wrong error messages would appear when using *gbak* with service_mgr.

fixed by V. Khorsun

~ ~ ~

SF #1122344 *gbak -kill* option would drop an existing shadow.

fixed by D. Yemanov

~ ~ ~

Not registered *gbak* was adding garbage bytes to the SPB when called in the -se[rvice_mgr] mode.

fixed by A. dos Santos Fernandes, C. Valderrama, V. Khorsun

~ ~ ~

gpre

SF #504978 gpre variable names were being truncated.

fixed by C. Valderrama

~ ~ ~

SF #527677 gpre "ANSI85 compatible COBOL" switch was broken.

fixed by C. Valderrama

~ ~ ~

SF #1103666 gpre was using inconsistent lengths

fixed by C. Valderrama

~ ~ ~

SF #1103670 gpre would invalidate a quoted cursor name after it was opened.

fixed by C. Valderrama

~ ~ ~

SF #1103683 gpre was not checking the length of the DB alias.

fixed by C. Valderrama

~ ~ ~

SF #1103740 gpre did not detect duplicate quoted cursor names

fixed by C. Valderrama

~ ~ ~

Not registered gpre could not generate more than 32,000 identifiers.

fixed by A. Harrison

~ ~ ~

gstat

Not registered Error output by *gstat* on Windows 32 was incorrect.

fixed by C. Valderrama

~ ~ ~

fb_lock_print

Not registered fb_lock_print could fail, with an exception message "*the requested operation cannot be performed on a file with a user-mapped section open.*"

fixed by V. Khorsun

~ ~ ~

Linux Installs

SF #1011401 The start/stop script was breaking halt/reboot on Slackware.

by A. Peshkov

~ ~ ~

Code Clean-up

(Not a bug) -L[ocal] command-line switch for SS on Win32 is gone

by D. Yemanov

~ ~ ~

Assorted clean-up

- Extensive, ongoing code cleanup and style standardization
- Broken write-ahead logging (WAL) and journalling code is fully cleaned out

by C. Valderrama

~ ~ ~

Platform-specific

Not registered (SuSE Linux) Service would not restart correctly on SuSE Linux.

by A. Peshkov

~ ~ ~

(CORE-839) (Windows) Instclient.exe failed to install gds32.dll over an existing version from V1.5.1 or later.

fixed by P. Reeves

~ ~ ~