IDA Pro 4.9 Service Pack

Major features

- Introduction of the debugger for Windows CE 5.0 for customers of the Windows CE/ARM Remote debugging module.

Bug Fixes

- The 'Window popup' keyboard key (F10) was not working in the disassembly listing window
- COM files were loaded at the segment 0 which made impossible to add PSP
- 64-bit debugging could fail with latest version of Windows XP Professional x64 Edition
- address expressions containing middle spaces were not parsed correctly in the 'jump to address' command.
- Alt-K was not closing dialog forms anymore
- AMD64: 16bit instructions with 66 prefix which are 64-bit by default were disassembled with the 66 prefix in a separate line
- any IDC error before a function definition might cause an access violation.
- ASCSTR_C was missing in idc.idc
- TMS320C55 binaries were loaded in little-endian mode; coff files were loaded correctly
- changing the target assembler could lead to a crash if the comment sequences for the current and new assemblers were of different length
- comments at the end of line in plugins.cfg were causing syntax errors
- the operand size of cwde was wrong (not visible in the listing)
- calling a synchronous command from a debugger notification handler was cancelling the eventual current asynchronous command.
- debugging for WinCE: if the input file was not present on the device and IDA proposed to copy it, and the user accepted, then the startup directory parameter would be set wrongly to the input file name. This does not really matter since this parameter was not used in WinCE (it has no concept of the current directory)
- deleting the last entries from the sorted problem list could cause an internal error.
- DelFunction(ea) where ea is not equal to the function beginning was not deleting the function from the list but was deleting the function description
- DLL rebasing was not working when attaching to a process
- create_flow_chart() could display wrong graph because function tail iterators could become invalid after several calls to the kernel. A workaround for this has been added in the form of reset_func() function
- gui: some options set in the classic 'load file' were not taken into account.
- The CommentEx() IDC function help page was wrong.
- The help pages erroneously stated that win32_remote uses -p switch for the password. It is -P.
- hex views and watches were not refreshed in the debugger
- IBM PC pop instruction was never using 'small' keyword

- IDA could endlessly loop during final pass of the analysis
- IDA was unable to copy the debugger server to WinCE 5.0 because this OS requires the numberOfWritten bytes parameter to CeWriteFile to be non zero
- IDA up to 4.9 was not saving ARM specific options in the database. The problem has been corrected the old databases use the default settings from the configuration files (as before)
- IDA was loading M68K COFF files with wrong byte endianness
- IDA was not automatically loading PDB information for 64-bit PE files (manually loading them was working)
- IDA was not aware that in the Watcom __fastcall calling convention a stack parameter prevents the remaining parameters to be passed in the registers
- IDA would complain that some manual operands did not match the original operand value
- ida_kdstub.dll was missing in the arm debugger
- idagui.cfg was missing some hotkey definitions
- IDC: it was impossible to use Comment() and RptCmt() functions
- IDC: SetDefReg() was truncating the register value to be 16-bits
- if the user refused to upgrade his database, temporary files were not deleted
- The input fields of the 'user defined offset' dialog box were cleared each time - this made it more difficult to use.
- It was impossible to delete the type of an unnamed item.
- It was impossible to patch an uninitialized byte with 0xFF
- It was impossible to start the debugger for a remote file with full path because the input file path would be stripped away
- The M68K module was erroneously complaining about missing names for near typed references
- The MIPS HI16 relocation was not handled properly in some cases. This fix is a best guess.
- The navigation band range was not refreshed when one database was closed and another opened
- NTSTATUS error codes were missing in ntddk.til and wdm.til
- PC: 8F D8 was incorrectly disassembled as an instruction; it is an invalid opcode
- PC: memory operand of "mov mem, segreg" is always 16-bit
- PC: movsxd instruction was disassembled as movsx (the difference is important for 16-bit source operand)
- PC: xchg rax, r15 was disassembled incorrectly
- The PE header segment would also contain the contents of the first segment.
- The PE loader could cause an access violation if the input file had wrong debug information offset.
- The PPC module was sign extending absolute addresses to 64-bit in the 64-bit version of IDA
- pro.h could not be used with VS2005
- processor specific options were not always correctly saved into the database
- rebasing the program could lead to access violations
- SDK: qvector assign() method was incorrect
- SDK: select_thread() was not working if called from a debugger notification handler
- segment names were not recognized in the 'jump to address' command
- struct and member repeatable comments were not displayed in structure variable definitions

- SUPER10: all jmpt instructions were disassembled with cc_UC condition
- The confirmation dialog box was not resized correctly for big fonts; the same problem with the chart builder plugin
- The exception code in the 'edit exception' dialog box was displayed incorrectly
- The types of local names were not displayed in the listing
- Unloading type information from the database to an idc file could produce wrong idc file in some cases (structure members of enum type would not have the closing quote after the enum name)
- the vc8extra.sig was named "VC7 Extra (technology) library"
- Very long comments (>1KB) were not correctly displayed
- Visual Studio 'vftable' mangled names were demangled incorrectly
- When converting operand types IDA was not considering ds:### numbers as immediate values which for example could lead to a strange selection of structure offset fields
- When detaching the debugger from a process ida would presume that detaching failed and not switch to normal desktop
- xrefs from structure instances to structure type definitions were not created for terse structures

Contact Information

© 2006 DataRescue SA/NV

40 Blvd Piercot

4000 Liège

Belgium

t - +32-4-3446510

f - +32-4-3446514

info@datarescue.com