Valgrinding Wine: Using Valgrind to find memory problems in Wine

Austin English
WineConf 2015
2015/09/20
Vienna, Austria
What is Valgrind

• Valgrind is a set of tools aimed at finding bugs and performance problems in programs. It shows reads of uninitialized memory, accesses to inaccessible memory, and memory leaks.

• Can be used in combination with the TestSuite to find problems in Wine's dlls/programs, as well as its tests

• http://valgrind.org/

• http://wiki.winehq.org/WineAndValgrind

• https://github.com/austin987/wine_misc/tree/master/valgrind
Statistics

- 316 open bugs
- 125 fixed bugs (with keyword*, maybe ~111 more)
- 419 commits attributed
  - Top authors:
    - 91 Nikolay Sivov
    - 57 Hans Leidekker
    - 41 Huw Davies
    - 35 Henri Verbeet

*As of 2015/09/16 - wine-1.7.51-181-g8fdcc23
Running Testsuite with Valgrind

- $ export OANOCACHE=1
- $ export VALGRIND_OPTS="-q --trace-children=yes --track-origins=yes --gen-suppressions=all
--suppressions=$WINESRC/tools/valgrind/valgrind-suppressions-external
--suppressions=$WINESRC/tools/valgrind/valgrind-suppressions-ignore $suppress_known $fatal_warnings --leak-check=full --num-callers=20 --workaround-gcc296-bugs=yes --vex-iropt-register-updates=allregs-at-mem-access"
- $ export WINETEST_TIMEOUT=600
- $ export WINE_HEAP_TAIL_REDZONE=32
- $ export WINETEST_WRAPPER=valgrind
- $ make -k test >> ${WINESRC}/logs/$version.log
Major Problems

• Since Mozilla upstream moved to using VS2013, using wine-gecko PDB builds hangs Wine (bug #38604)
• VS2013 PDBs don't work with wine's dbghelp (bug #38594, bug #37746)
• Crashes Xorg with Nouveau (fd.o bug #91972)
• MacOSX doesn't work at all (kde bug #349804)
• Lots of valgrind issues with OpenGL drivers (i965/nvidia...)
Contributing

- Fix Wine's valgrind issues, there are plenty to choose from ;)
- Improve Wine's dbghelp / winedbg for VS2013
- Fix crashing (13) / hanging (4) / failing (24) tests
Win64

- Mostly untested, on my backburner
- One fixed bug (with ~4600 occurrences in the tests, bug #38695), fixed by:

  **commit**
  885394bb0ae83925f57c9066da2d06f6e011fa17

  **Author:** Nikolay Sivov
  <nsivov@codeweavers.com>

  **Date:**   Sun Jun 21 09:03:54 2015 +0300

  **gdi32/freetype:** Properly handle loading of **FT_Long-sized** types (Valgrind).
Questions?

• Thanks for your time and attention