

Ryzom - Bug # 1065

Status:	New	Priority:	Normal
Author:	Enoril	Category:	
Created:	08/06/2010	Assignee:	
Updated:	07/10/2011	Due date:	
Subject:	ryzom_client crash under linux when going from live shard to ring shard		
Description	<p>The client crash (seg fault) when switching from the live shard to ring shard via the "Scenario Editor" button found</p> <p>You will find below the trace of this crash:</p> <p>@</p> <p>Program received signal SIGSEGV, Segmentation fault.</p> <p>0x0031e7c9 in glDisable () from /usr/lib/nvidia-current/libGL.so.1</p> <p>(gdb) bt</p> <p>#0 0x0031e7c9 in glDisable () from /usr/lib/nvidia-current/libGL.so.1</p> <p>#1 0x08e5b80f in NL3D::CDriverUser::setupMatrixContext() ()</p> <p>#2 0x08e5df7d in NL3D::CDriverUser::setMatrixMode2D(NL3D::CFrustum const&) ()</p> <p>#3 0x08e5b2f9 in NL3D::UDriver::setMatrixMode2D11() ()</p> <p>#4 0x08610da2 in CProgress::internalProgress(float) ()</p> <p>#5 0x084c79a0 in CFarTP::disconnectFromPreviousShard() ()</p> <p>#6 0x084cc2c6 in CLoginStateMachine::run() ()</p> <p>#7 0x0953e322 in NLMISC::TCoTaskData::run() ()</p> <p>#8 0x09512e47 in ?? ()</p> <p>#9 0x0013396e in start_thread () from /lib/tls/i686/cmov/libpthread.so.0</p> <p>#10 0x00533a0e in clone () from /lib/tls/i686/cmov/libc.so.6</p> <p>@</p> <p>i'm using the Official Ryzom Client for GNU/Linux (rev 551 apparently) in the official server (aniro)</p>		

History

#1 - 07/08/2011 10:51 pm - piglop

It also happens when you're in game and you exit to character selection.

#2 - 07/08/2011 11:43 pm - rti

Probably related to #1175 and #1270

In #1175 naush provided a patch.

#3 - 07/10/2011 03:04 pm - piglop

Indeed. And I confirm the patch fixes the segfault. Exiting to character selection works fine now.

But when entering a ring, there's now a new segfault:

Program received signal SIGSEGV, Segmentation fault.

0x0826d3f3 in ucstring::toUtf8 (this=0x1a3bb360)

at /home/mike/devel/ryzom/ryzom/code/nel/include/nel/misc/ucstring.h:157

157 if (*first < 0x80)

(gdb) bt

#0 0x0826d3f3 in ucstring::toUtf8 (this=0x1a3bb360)

at /home/mike/devel/ryzom/ryzom/code/nel/include/nel/misc/ucstring.h:157

#1 0x086c3883 in invoke_member<std::basic_string<char> (ucstring::*)() const, boost::mpl::vector2<std::basic_string<char>, ucstring const&>, luabind::detail::null_type> (L=0x116d41d8) at /usr/include/luabind/detail/call.hpp:283

#2 invoke0<std::basic_string<char> (ucstring::*)() const, boost::mpl::vector2<std::basic_string<char>, ucstring const&>, luabind::detail::null_type, boost::is_void<std::basic_string<char> > > (L=0x116d41d8)

at /usr/include/luabind/detail/call.hpp:78

#3 invoke<std::basic_string<char> (ucstring::*)() const, boost::mpl::vector2<std::basic_string<char>, ucstring const&>, luabind::detail::null_type> (

L=0x116d41d8) at /usr/include/luabind/detail/call.hpp:101

#4 luabind::detail::function_object_impl<std::basic_string<char>, std::char_traits<char>, std::allocator<char> > (ucstring::*)() const, boost::mpl::vector2<std::basic_string<char>, std::char_traits<char>, std::allocator<char> >, ucstring const&>, luabind::detail::null_type>::entry_point (L=0x116d41d8)

at /usr/include/luabind/make_function.hpp:63

#5 0xb6c672ea in ?? () from /usr/lib/liblua5.1.so.0

#6 0xb6c7245a in ?? () from /usr/lib/liblua5.1.so.0

#7 0xb6c677d0 in ?? () from /usr/lib/liblua5.1.so.0

#8 0xb6c62771 in ?? () from /usr/lib/liblua5.1.so.0

#9 0xb6c66df3 in ?? () from /usr/lib/liblua5.1.so.0

#10 0xb6c66e55 in ?? () from /usr/lib/liblua5.1.so.0

#11 0xb6c62598 in lua_pcall () from /usr/lib/liblua5.1.so.0

#12 0x0866dcfe in pcall (this=0xfb3a2e0, code=..., dbgSrc=..., numRet=0)

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/interface_v3/lu_helper_inline.h:462

#13 CLuaState::executeScriptInternal (this=0xfb3a2e0, code=..., dbgSrc=..., numRet=0)

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/interface_v3/lu_helper.cpp:355

#14 0x0866e088 in CLuaState::executeFile (this=0xfb3a2e0, pathName=...)

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/interface_v3/lu_helper.cpp:423

#15 0x089fb477 in R2::CEditor::doLuaScript (this=0xaa494f8,

filename=0x8b03950 "r2_core.lua",

fileDescText=0x8b027b8 "r2ed common functions and definitions")

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/r2/editor.cpp:4410

#16 0x08a1725f in R2::CEditor::init (this=0xaa494f8,

initialMode=R2::CEditor::AnimationModeDm, accessMode=R2::CEditor::AccessDM)

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/r2/editor.cpp:2659

#17 0x08a17e16 in R2::CEditor::autoConfigInit (this=0xaa494f8,

serverIsRingSession=true)

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/r2/editor.cpp:362

#18 0x082a4792 in mainLoop ()

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/main_loop.cpp:2961

#19 0x08400d7a in main (argc=Cannot access memory at address 0xc0000000

)

at /home/mike/devel/ryzom/ryzom/code/ryzom/client/src/client.cpp:618