Wt - Bug #4989

Wt 3.3.5 segfaults on nmap scan

06/20/2016 06:24 PM - Martin Dyring-Andersen

Status:	Closed	**Start date:**	06/20/2016
Priority:	High	**Due date:**	
Assignee:	Roel Standaert	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	3.3.6		

Description

Running nmap 6.47 with arguments -A -T4 results in a segfault. This is with a dummy application (no widgets loaded), so should be easily reproducible.

Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt25-2 (2016-04-08) x86_64 GNU/Linux

Stack trace:

Program received signal SIGSEGV, Segmentation fault.

[Switching to Thread 0x7f4ac60c8700 (LWP 25894)]

Wt::WebSession::checkTimers (this=0x7f4aa0004130) at /opt/test/src/dependencies/wt/src/web/WebSession.C:704

704 const std::vector<WWidget *>& timerWidgets = timers->children();

(gdb) bt

#0 Wt::WebSession::checkTimers (this=0x7f4aa0004130) at /opt/test/src/dependencies/wt/src/web/WebSession.C:704

#1 0x00000000007be40d in Wt::WebSession::render (this=0x7f4aa0004130, handler=...) at /opt/test/src/dependencies/wt/src/web/WebSession.C:2600

#2 0x00000000007c28e8 in Wt::WebSession::Handler::~Handler (this=0x7f4ac60c5c20, __in_chrg=) at /opt/test/src/dependencies/wt/src/web/WebSession.C:1035

#3 0x00000000007aae66 in Wt::WebController::handleRequest (this=0x17213b0, request=0x7f4aa0003f60) at /opt/test/src/dependencies/wt/src/web/WebController.C:733

#4 0x000000000086ecbc in operator() (a1=0x7f4aa0003f60, p=0x17213b0, this=) at /opt/test/src/dependencies/install/include/boost/bind/mem_fn_template.hpp:165

#5 operator()<boost::_mfi::mf1<void, Wt::WebController, Wt::WebRequest*>, boost::_bi::list0> (a=, f=, this=) at /opt/test/src/dependencies/install/include/boost/bind/bind.hpp:319

#6 operator() (this=) at /opt/test/src/dependencies/install/include/boost/bind/bind.hpp:1222

#7 asio_handler_invoke<boost::_bi::bind_t<void, boost::_mfi::mf1<void, Wt::WebController, Wt::WebRequest*, boost::_bi::list2<boost::_bi::value<Wt::WebController>, boost::_bi::value<http::server::HTTPRequest*> > > > (

function=) at /opt/test/src/dependencies/install/include/boost/asio/handler_invoke_hook.hpp:69

#8 invoke<boost::_bi::bind_t<void, boost::_mfi::mf1<void, Wt::WebController, Wt::WebRequest, boost::_bi::list2<boost::_bi::value<Wt::WebController>, boost::_bi::value<http::server::HTTPRequest*> > >, boost::_bi::bind_t<void, boost::_mfi::mf1<void, Wt::WebController, Wt::WebRequest, boost::_bi::list2<boost::_bi::value<Wt::WebController>, boost::_bi::value<http::server::HTTPRequest*> > > > (context=, function=)

at /opt/test/src/dependencies/install/include/boost/asio/detail/handler_invoke_helpers.hpp:37

#9 boost::asio::detail::completion_handler<boost::_bi::bind_t<void, boost::_mfi::mf1<void, Wt::WebController, Wt::WebRequest, boost::_bi::list2<boost::_bi::value<Wt::WebController*>, boost::_bi::value<http::server::HTTPRequest*> > > >::do_complete (owner=0x1721920, base=) at /opt/test/src/dependencies/install/include/boost/asio/detail/completion_handler.hpp:68

#10 0x000000000081d288 in complete (bytes_transferred=, ec=..., owner=..., this=) at /opt/test/src/dependencies/install/include/boost/asio/detail/task_io_service_operation.hpp:38

#11 do_run_one (ec=..., this_thread=..., lock=..., this=0x1721920) at /opt/test/src/dependencies/install/include/boost/asio/detail/impl/task_io_service.ipp:372

#12 boost::asio::detail::task_io_service::run (this=0x1721920, ec=...) at /opt/test/src/dependencies/install/include/boost/asio/detail/impl/task_io_service.ipp:149

#13 0x000000000081aeb4 in run (this=0x1721e18) at /opt/test/src/dependencies/install/include/boost/asio/impl/io_service.ipp:59

#14 Wt::WIOService::run (this=0x1721e10) at /opt/test/src/dependencies/wt/src/Wt/WIOService.C:180

#15 0x00000000008b7460 in thread_proxy ()

#16 0x00007f4ac7c7f0a4 in start_thread (arg=0x7f4ac60c8700) at pthread_create.c:309

#17 0x00007f4ac79b487d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111

History

#1 - 06/21/2016 10:51 AM - Koen Deforche

- Status changed from New to InProgress

- Assignee set to Roel Standaert

#2 - 06/21/2016 03:49 PM - Roel Standaert

- Status changed from InProgress to Implemented @Emweb

#3 - 06/22/2016 09:53 AM - Koen Deforche

- Status changed from Implemented @Emweb to Resolved

#4 - 07/13/2016 05:07 PM - Koen Deforche

- Status changed from Resolved to Closed

- Target version set to 3.3.6