Wt - Bug #8391

Crash in active Wt::Http::Client destructor if started outside WApplication

04/21/2021 04:10 PM - Dries Mys

Status:	Resolved	**Start date:**	04/21/2021
Priority:	Normal	**Due date:**	
Assignee:	Roel Standaert	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	4.6.0		

Description

Crash reason

The destructor of Http::Client calls abort which asynchronously aborts the http request.

If impl->hasServer() is false, a pointer to the Client's impl_ member is passed to asyncStop; see
https://github.com/emweb/wt/blob/master/src/Wt/Http/Client.C#L850
This member will be destructed briefly after this call, as abort is called from inside the Http::Client destructor.
However, in the asynchronously executed stop function (https://github.com/emweb/wt/blob/master/src/Wt/Http/Client.C#L178), this (possibly) dangling pointer will be dereferenced.

Note that this code was added in commit 9c44b4e3c2 with commit message "Fixed possible race condition when resetting impl_ of HTTP Client". However it is unclear to me which in which scenario the mentioned race condition is avoided.

Steps to reproduce the issue

1. Start a new thread
2. Start a (long running) http request using Wt::Http::Client
3. Destruct the Wt::Http::Client object (before the http request is finished.

History

#1 - 08/09/2021 11:40 AM - Roel Standaert

- Status changed from New to InProgress

- Assignee set to Roel Standaert

- Target version set to 4.6.0

#2 - 08/09/2021 11:52 AM - Roel Standaert

- File issue_8391.cpp added

Added a simple test that reproduces this issue when built with address sanitizer.

#3 - 08/19/2021 04:29 PM - Roel Standaert

- Status changed from InProgress to Review

#4 - 08/24/2021 06:31 PM - Roel Standaert

- Status changed from Review to Implemented @Emweb

#5 - 08/24/2021 06:38 PM - Roel Standaert

- % Done changed from 0 to 100

#6 - 08/24/2021 06:38 PM - Roel Standaert

- Status changed from Implemented @Emweb to Resolved

Files

issue_8391.cpp	210 Bytes	08/09/2021	Roel Standaert