Quassel IRC - Bug #1314

Crash

09/27/2014 01:59 PM - pucilowski

Status: Resolved Start date: 09/27/2014

Priority: Immediate Due date:

Assignee: % Done: 100%

Category: Estimated time: 0.00 hour

Target version:

Version: 0.10.0 OS: Any

Description

Error: ASSERT: "uint(i) < uint(size())" in file /usr/include/qt4/QtCore/qbytearray.h, line 414</pre>

It happens as a result of receiving a very long line of input on a fishlim enabled channel.

An example of such line was the following at 284 characters.

Related issues:

Related to Quassel IRC - Bug #1059: core crashes on not decryptable text Resolved 03/03/2011

Associated revisions

Revision 8b5ecd22 - 10/21/2014 09:20 PM - Manuel Nickschas

Check for invalid input in encrypted buffers

The ECB Blowfish decryption function assumed that encrypted input would always come in blocks of 12 characters, as specified. However, buggy clients or annoying people may not adhere to that assumption, causing the core to crash while trying to process the invalid base64 input.

With this commit we make sure that we're not overstepping the bounds of the input string while decoding it; instead we bail out early and display the original input. Fixes #1314.

Thanks to Tucos for finding that one!

Revision 6b2d80b8 - 10/21/2014 09:38 PM - Manuel Nickschas

Check for invalid input in encrypted buffers

The ECB Blowfish decryption function assumed that encrypted input would always come in blocks of 12 characters, as specified. However, buggy clients or annoying people may not adhere to that assumption, causing the core to crash while trying to process the invalid base64 input.

With this commit we make sure that we're not overstepping the bounds of the input string while decoding it; instead we bail out early and display the original input. Fixes #1314.

Thanks to Tucos for finding that one!

History

#1 - 10/21/2014 09:30 PM - Anonymous

- Status changed from New to Resolved
- % Done changed from 0 to 100

Applied in changeset <u>quassel|8b5ecd226f9208af3074b33d3b7cf5e14f55b138</u>.

05/01/2024 1/2

#2 - 09/08/2018 01:16 AM - genius3000

- Related to Bug #1059: core crashes on not decryptable text added

05/01/2024 2/2