Starred by 3 users

Owner:	----
CC:	rlohn...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Apr 6, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-qt
Reported-2020-01-31
Disclosure-2020-04-30

Issue 20450: qt:setMarkdown: Heap-use-after-free in QScopedPointer<QObjectData, QScopedPointerDeleter<QObjectData> >::operator->

Reported by ClusterFuzz-External on Fri, Jan 31, 2020, 7:27 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5728348359884800

Project: qt
Fuzzing Engine: libFuzzer
Fuzz Target: setMarkdown
Job Type: libfuzzer_asan_qt
Platform Id: linux

Crash Type: Heap-use-after-free READ 8
Crash Address: 0x6020000006d8
Crash State:
  QScopedPointer<QObjectData, QScopedPointerDeleter<QObjectData> >::operator->
  QTextList::count
  QTextMarkdownImporter::insertBlock

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_qt&range=202001300747:202001310627

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5728348359884800

Issue filed automatically.

See https://google.github.io/oss-fuzz/advanced-topics/reproducing for instructions to reproduce this bug locally.
When you fix this bug, please
  * mention the fix revision(s).
  * state whether the bug was a short-lived regression or an old bug in any stable releases.
  * add any other useful information.
This information can help downstream consumers.

If you need to contact the OSS-Fuzz team with a question, concern, or any other feedback, please file an issue at https://github.com/google/oss-fuzz/issues. Comments on individual Monorail issues are not monitored.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse
without an upstream patch, then the bug report will automatically
become visible to the public.

Comment 1 by rlohn...@gmail.com on Fri, Jan 31, 2020, 10:23 AM EST

Reported to security@qt-project.org on January 31st.

Comment 2 by sheriffbot@chromium.org on Fri, Jan 31, 2020, 1:22 PM EST Project Member

Labels: Disclosure-2020-04-30

Comment 3 by rlohn...@gmail.com on Wed, Feb 12, 2020, 11:57 AM EST

Cannot reproduce with Qt 5.14.0.

Comment 4 by rlohn...@gmail.com on Thu, Feb 13, 2020, 8:39 AM EST

Affects Qt 5.14.1.

Comment 5 by ClusterFuzz-External on Thu, Mar 5, 2020, 5:00 AM EST Project Member

Status: Verified (was: New)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5728348359884800 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_qt&range=202003040431:202003050424

If this is incorrect, please file a bug on https://github.com/google/oss-fuzz/issues/new

Comment 6 by rlohn...@gmail.com on Thu, Mar 5, 2020, 7:23 AM EST

Fixed in qtbase by 7447e2b337f12b4d04935d0f30fc673e4327d5a0
https://codereview.qt-project.org/c/qt/qtbase/+/291706

Comment 7 by sheriffbot on Sat, Apr 4, 2020, 2:51 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed for 30 days. It has been opened to the public.

- Your friendly Sheriffbot

Comment 8 by rlohn...@gmail.com on Mon, Apr 6, 2020, 2:13 PM EDT

Fixed in Qt 5.14.2.
There, the testcase triggers https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=21563 instead.