QTBUG-81272

Qt tries to load invalid library from CWD

Details

Type:	Bug	Status:	CLOSED
Priority:	P1: Critical	Resolution:	Done
Affects Version/s:	5.13.1, 5.14.0	Fix Version/s:	5.12.7, (2)
Component/s:	Core: Plugins		
Labels:	None		
Platform/s:	Linux/X11		
Commits:	e6f1fde24f77f63fb16b2df239f82a89d2bf05dd (qt/qtbase/5.14.1) eb192256e74ba46e719fcadcb962592d19612f6e (qt/qtbase/5.12.7)		

Description

With strace, it is visible that Qt (installed in /usr/lib64) tries to load a plugin relative to the current directory:

```
~> strace -fefile qdbusviewer |& grep -i hasw
[pid  3055] openat(AT_FDCWD, "haswell/libXcursor.so.1", O_RDONLY|O_CLOEXEC) = -1 ENOENT (Datei oder Verzeichnis nicht gefunden)
[pid  3055] openat(AT_FDCWD, "haswell/libXcursor", O_RDONLY|O_CLOEXEC) = -1 ENOENT (Datei oder Verzeichnis nicht gefunden)
```

This is undesirable as the CWD contents can be unknown, so it might be finding something which it's not supposed to.

Gerrit Reviews

No reviews matched the request. Check your Options in the drop-down menu of this sections header.

Activity

Fabian Vogt added a comment - 09 Jan '20 16:29

Backtrace:

```
#0  QLibraryPrivate::load_sys (this=this@entry=0x5555555afbd0) at plugin/qlibrary_unix.cpp:222
#1  0x00007ffff6dba6a8 in QLibraryPrivate::load (this=0x5555555afbd0) at plugin/qlibrary.cpp:553
#2  QLibrary::load (this=<optimized out>) at plugin/qlibrary.cpp:808
#3  0x00007ffff3ca1950 in ?? () from /usr/lib64/libQt5XcbQpa.so.5
#4  0x00007ffff3c8e20d in QXcbScreen::QXcbScreen(QXcbConnection*, QXcbVirtualDesktop*, unsigned int, xcb_randr_get_output_info_reply_t*, xcb_xinerama_screen_info_t const*, int) () from /usr/
#5  0x00007ffff3cae65b in QXcbConnection::initializeScreens() () from /usr/lib64/libQt5XcbQpa.so.5
```

It seems to be caused by the unconditional prefixing of paths with `haskell/`, which also applies to an empty path.

Thiago Macieira added a comment - 10 Jan '20 16:41

Raising to P1, this is potentially a security issue.

People

Assignee:

Thiago Macieira

Reporter:

Fabian Vogt

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

Dates

Created:

09 Jan '20 16:28

Updated:

29 Jan '20 07:02

Resolved:

18 Jan '20 15:58

Gerrit Reviews

There are no open Gerrit changes

There are 3 closed Gerrit changes

There are 3 closed Gerrit changes

QLibrary/Unix: do not attempt to load a library relative to $PWD

QLibrary/Unix: do not attempt to load a library relative to $PWD

QLibrary/Unix: do not attempt to load a library relative to $PWD