Obsolete Bug P3 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION su...@gmail.com created issue #1 Nov 8, 2013 02:42PM

In china,use CMCC SIM, first login the Linxi.apk(com.iflytek.cmcc),and say "充话费"。
The app will jump to another page to charge fee.If the phone time is not agree to the net time and this operation is the first,NE will happen by chance.

Build fingerprint: 'OPPO/OPPO82_13067/OPPO82_13067:4.2.2/JDQ39/1381940340:eng/test-keys'
pid: 1414, tid: 1966, name: WebViewCoreThre >>> com.iflytek.cmcc <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr deadbaad
r0 00000000 r1 00000027 r2 deadbfff r3 00000000
r4 00000000 r5 60189694 r6 000449dc r7 6349d03f
r8 400dbca0 r9 000017f5 sl 00000050 fp 60189794
ip 00000001 sp 60189690 lr 400a8a30 pc 400a2238 cpsr 60000010

backtrace:
#00 pc 0002a238 /system/lib/libc.so
#01 pc 00020414 /system/lib/libc.so (dlfree+7988)
#02 pc 0001c57c /system/lib/libc_malloc_debug_mtk.so (mtk_free+128)
#03 pc 0000e0f0 /system/lib/libc.so (free+16)
#04 pc 003bb045 /system/lib/libwebcore.so
#05 pc 003bb189 /system/lib/libwebcore.so
#06 pc 00126aed /system/lib/libwebcore.so
#07 pc 00175c3f /system/lib/libwebcore.so
#08 pc 00175f69 /system/lib/libwebcore.so
#09 pc 00176e81 /system/lib/libwebcore.so
#10 pc 003ba1b9 /system/lib/libwebcore.so
#11 pc 0017d6a1 /system/lib/libwebcore.so
#12 pc 003bc463 /system/lib/libwebcore.so
#13 pc 003bc893 /system/lib/libwebcore.so
#14 pc 003bc933 /system/lib/libwebcore.so
#15 pc 003bd049 /system/lib/libwebcore.so
#16 pc 003bcc2d /system/lib/libwebcore.so
#17 pc 0013cb39 /system/lib/libwebcore.so
#18 pc 001a3e1d /system/lib/libwebcore.so
#19 pc 002ac983 /system/lib/libwebcore.so
#20 pc 0001df90 /system/lib/libdvm.so (dvmPlatformInvoke+112)
#21 pc 00062b00 /system/lib/libdvm.so (dvmCallJNIMethod(unsigned int const*, JValue*, Method const*, Thread*)+568)
#22 pc 000273a0 /system/lib/libdvm.so
#23 pc 0002b2dc /system/lib/libdvm.so (dvmInterpret(Thread*, Method const*, JValue*)+180)
#24 pc 00084a8c /system/lib/libdvm.so (dvmCallMethodV(Thread*, Method const*, Object*, bool, JValue*, std::__va_list)+400)
#25 pc 00084b18 /system/lib/libdvm.so (dvmCallMethod(Thread*, Method const*, Object*, JValue*, ...)+36)
#26 pc 000700f8 /system/lib/libdvm.so
#27 pc 0000f65c /system/lib/libc.so (__thread_entry+72)

This is because one chunk of memory has been freed but be used again.The chunk structure is destroyed.
The Stacks which destroys the memory is :

libwebcore.so scoped_refptr<>::operator=(参数1:0x60BE6000, 参数4:1) + 14 <external/chromium/base/memory/ref_counted.h:277>
libwebcore.so android::WebUrlLoaderClient::didFail() + 68 <external/webkit/Source/WebKit/android/WebCoreSupport/WebUrlLoaderClient.cpp:432>
libwebcore.so RunnableMethod<>::Run(参数1:0x5EAE8FD8, 参数2:0x61C9AA60, 参数3:0x5E21855D, 参数4:0) + 58 <external/chromium/base/tuple.h:551>
libwebcore.so android::(anonymous namespace)::RunTask(参数1:0x5EAE8FD8) + 8 <external/webkit/Source/WebKit/android/WebCoreSupport/WebUrlLoaderClient.cpp:348>
libwebcore.so WTF::dispatchFunctionsFromMainThread(参数1:0, 参数4:0x5E891BA4) + 104 <external/webkit/Source/JavaScriptCore/wtf/MainThread.cpp:155>
libwebcore.so android::JavaSharedClient::ServiceFunctionPtrQueue(参数4:0x5A8A2E10) + 56 <external/webkit/Source/WebKit/android/jni/JavaSharedClient.cpp:134>

Reporter su...@gmail.com
Type Bug
Priority P3
Severity S3
Status Won't fix (Obsolete)
Access Default access View
Assignee --
Verifier --
Collaborators
CC
su...@gmail.com
AOSP ID 61958
ReportedBy Developer
Found In --
Targeted To --
Verified In --
In Prod

That's because function finish in WebUrlLoaderClient.cpp。
When m_resourceHandle = 0 cause WebUrlLoader's deconstruct function is called ,then the WebUrlLoaderClient's deconstruct function is called. But the finish has not end,and then WebUrlLoaderClient is still used.

Thanks

COMMENTS

All comments ▾ ↓ Oldest first

hb...@gmail.com <hb...@gmail.com> #2 Nov 9, 2013 04:40AM

Can you reproduce this in the latest 4.4 emulator or devices..? The Android webview has been *completely* changed and may very well respond differently now.

en...@google.com <en...@google.com> Dec 8, 2014 11:57AM

Status: Won't Fix (Obsolete)