Emulator - Emulator Issues #12257

Driver: San Francisco Broadcasts "NTRJ41", Crashing/Reading Invalid Memory

09/12/2020 02:54 PM - JMC4789

Status:	Fixed	**% Done:**	0%
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Operating system:	N/A	**Relates to performance:**	No
Issue type:	Bug	**Easy:**	No
Milestone:		**Relates to maintainability:**	No
Regression:	No	**Regression start:**	
Relates to usability:	No	**Fixed in:**	5.0-13447

Description

Game Name?

Driver: San Francisco

Game ID? (right click the game in the game list, Properties, Info tab)

SDEV41 and NTRJ41 for the DS program

MD5 Hash? (right click the game in the game list, Properties, Verify tab, Verify Integrity button)

dd3e040f9aeb20f581b209830e2d5cfb

What's the problem? Describe what went wrong.

When starting up a new game, Driver: San Francisco will broadcast NTRJ41 for DSes to take control of a second player and control the shooting more accurately. Dolphin promptly dies if MMU is enabled with this logging.

40:25:373 Core\HW\DVD\FileMonitor.cpp:87 W[FileMon]: 72,396 kB Cities/san_francisco.d4c
40:25:389 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: MPDL| now starting to broadcast DS-program...
40:25:389 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: MPDL|
40:25:390 Core\IOS\IOS.cpp:524 I[IOS]: Opening /dev/net/kd/request (mode 0, fd 7)
40:25:391 Core\IOS\Network\KD\NetKDRequest.cpp:42 I[IOS_WC24]: NET_KD_REQ: IOCTL_NWC24_SUSPEND_SCHEDULAR - NI
40:25:392 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: << RVL_SDK - NCD release build: Jun 9 2009 11:59:48 (0x4199_60831) >>
40:25:392 Core\IOS\IOS.cpp:524 I[IOS]: Opening /dev/net/ncd/manage (mode 0, fd 7)
40:25:420 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: Unhandled Exception 2
40:25:420 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ------------------------- Context 0x807c3f18 -------------------------
40:25:420 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r0 = 0x00000003 (3) r16 = 0x00000000 (0)
40:25:421 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r1 = 0x8083ed68 (-2138837656) r17 = 0x00000000 (0)
40:25:421 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r2 = 0x8082e9e0 (-2138904096) r18 = 0x00000000 (0)
40:25:421 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r3 = 0x00000000 (0) r19 = 0x00000000 (0)
40:25:422 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r4 = 0x00000001 (1) r20 = 0x00000000 (0)
40:25:422 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r5 = 0x00000000 (0) r21 = 0x8069c19e (-2140552802)
40:25:422 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r6 = 0x00000001 (1) r22 = 0x802db294 (-2144488812)
40:25:423 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r7 = 0x00000000 (0) r23 = 0x8069fffa (-2140536838)
40:25:423 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r8 = 0x00000000 (0) r24 = 0x806a73e4 (-2140507164)

40:25:423 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r9 = 0x809ceb10 (-2137199856) r25 = 0x8074ea00 (
-2139821568)
40:25:423 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r10 = 0x8083ee38 (-2138837448) r26 = 0x8083ef38 (
-2138837192)
40:25:424 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r11 = 0x8083ee48 (-2138837432) r27 = 0x80742a00 (
-2139870720)
40:25:424 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r12 = 0x802da8ac (-2144491348) r28 = 0x8074ea04 (
-2139821564)
40:25:425 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r13 = 0x80828f60 (-2138927264) r29 = 0x80a16fc0 (
-2136903744)
40:25:425 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r14 = 0x802db268 (-2144488856) r30 = 0x80a16fc0 (
-2136903744)
40:25:425 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: r15 = 0x00000000 (0) r31 = 0x00000001 (1)
40:25:425 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: LR = 0x80380bac CR = 0x48000488
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: SRR0 = 0x8069475c SRR1 = 0x0000a032
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: GQRs----------
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: gqr0 = 0x00000000 gqr4 = 0x00060006
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: gqr1 = 0x00000000 gqr5 = 0x00070007
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: gqr2 = 0x00040004 gqr6 = 0x00000000
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: gqr3 = 0x00050005 gqr7 = 0x00000000
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:426 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: FPRs----------
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr0 = 0 fr1 = 0
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr2 = 0 fr3 = 0
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr4 = 0 fr5 = 0
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr6 = 0 fr7 = 0
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr8 = 320 fr9 = 0
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr10 = 16777216 fr11 = 1
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr12 = 2 fr13 = 0
40:25:427 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr14 = 0 fr15 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr16 = 0 fr17 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr18 = 0 fr19 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr20 = 0 fr21 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr22 = 0 fr23 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr24 = 0 fr25 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr26 = 0 fr27 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr28 = 0 fr29 = -1
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: fr30 = 0 fr31 = 0
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:428 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: PSFs----------
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps0 = 0x0 ps1 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps2 = 0x0 ps3 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps4 = 0x0 ps5 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps6 = 0x0 ps7 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps8 = 0xffffffff ps9 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps10 = 0xffffffff ps11 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps12 = 0x2 ps13 = 0x0
40:25:429 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps14 = 0x0 ps15 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps16 = 0x0 ps17 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps18 = 0x0 ps19 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps20 = 0x0 ps21 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps22 = 0x0 ps23 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps24 = 0x0 ps25 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps26 = 0x0 ps27 = 0x0
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps28 = 0x0 ps29 = 0xffffffff
40:25:430 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: ps30 = 0x0 ps31 = 0x0
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: Address: Back Chain LR Save
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083ed68: 0x8083ed88 0x80a16330
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083ed88: 0x8083ee48 0x8037f418
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083ee48: 0x8083ee68 0x8024910c
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083ee68: 0x8083eef8 0x802dbab0
40:25:431 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083eef8: 0x8083f008 0x802db6fc
40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083f008: 0x8083f078 0x802db2c0

40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083f078: 0x8083f098 0x802e1450
40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: 0x8083f098: 0xffffffff 0x80006474
40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: DSISR = 0x42000000 DAR = 0x00000058
40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: TB = 0x008cfbb42755adda
40:25:432 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:433 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: Instruction at 0x8069475c (read from SRR0) attempted to access invalid address 0x58 (read from DAR)
40:25:433 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]:
40:25:433 Core\HW\EXI\EXI_DeviceIPL.cpp:306 N[OSREPORT]: Last interrupt (19): SRR0 = 0x8023194c TB = 0x008cfbb42755ab00

If you disable MMU emulation, you can avoid the crash but the game will run extremely slow as Dolphin is peppered with a loop of invalid reads.

18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000058, PC = 0x8069475c
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x0000005c, PC = 0x80694768
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000090, PC = 0x80694784
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x000000c4, PC = 0x806947a4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x000000f8, PC = 0x806947c4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x0000012c, PC = 0x806947e4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000160, PC = 0x80694768
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000194, PC = 0x80694784
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x000001c8, PC = 0x806947a4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x000001fc, PC = 0x806947c4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000230, PC = 0x806947e4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000264, PC = 0x80694768
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000298, PC = 0x80694784
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x000002cc, PC = 0x806947a4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000300, PC = 0x806947c4
18:54:531 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000334, PC = 0x806947e4
18:54:556 Common\MsgHandler.cpp:115 E[MASTER]: Question: Invalid read from 0x00000058, PC = 0x8069475c

This is likely it trying to communicate with a DS.

What steps will reproduce the problem?

Start up Driver San Francisco.
Create a Profile if you haven't.
Start up Story mode.
Wait for it to load.
At the end of loading, you will get invalid reads or a crash depending on MMU settings.

Is the issue present in the latest development version? For future reference, please also write down the version number of the latest development version.

5.0-12581

Is the issue present in the latest stable version?

Yes, Dolphin 5.0

What are your PC specifications? (CPU, GPU, Operating System, more)

Core i7-6700K
Geforce GTX 1070
Windows 10

Is there anything else that can help developers narrow down the issue? (e.g. logs, screenshots, configuration files, savefiles, savestates)

Logs have been posted in the issue report above. You do not need any special saves/configurations to trigger this.

Related issues:

Related to Emulator - Emulator Issues #11977: Tales of Graces crashes attempt...	**Accepted**

History

#1 - 12/02/2020 07:54 PM - leoetlino

- Status changed from New to Fix pending

As expected, this is an IOS HLE bug.

https://github.com/dolphin-emu/dolphin/pull/9300

#2 - 12/02/2020 07:56 PM - leoetlino

- Related to Emulator Issues #11977: Tales of Graces crashes attempting to initiate DS communications added

#3 - 12/02/2020 07:56 PM - leoetlino

This is related to issue 11977, but ToG will not be fixed by PR 9300 as it likely requires more commands to be implemented and/or fixing more stuff.

#4 - 01/15/2021 11:13 PM - ZephyrSurfer

This PR has been merged.

Dolphin 5.0-13447 -> https://dolphin-emu.org/download/dev/27013e8d184a956090ec3299e2136cc6665df89f/

#5 - 01/16/2021 10:52 AM - JosJuice

- Fixed in set to 5.0-13447

- Status changed from Fix pending to Fixed