Emulator - Emulator Issues #12727

Mac builds crash when starting a game when using the ARM64 JIT recompiler

11/08/2021 03:50 AM - friendsxix

Status:	New	**% 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:**	

Description

Game Name?

Tested with both Animal Crossing and The Legend of Zelda: Twilight Princess.

Game ID?

GZ2E01 and GAFE01.

MD5 Hash?

41deff9b1fd2831f48fbfa2dd1054e4d for Twilight Princess. Animal Crossing is trimmed, but both games crash in exactly the same way.

What's the problem? Describe what went wrong.

Dolphin crashes immediately when attempting to start a game. The crash does not occur when using either the interpreter or the cached interpreter. Interestingly, the last build to not crash is 5.0-14274 (the last build before support for ARM-based Macs was added). Later builds crash even when running through Rosetta 2. Perhaps this is an issue with the M1 Max specifically? I do not have an M1 Pro machine to test. I have tried nuking Dolphin's settings in ~/Library/Application Support between tests to no avail.

What steps will reproduce the problem?

1) Open ROM
2) Crash.

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

Yes, tested on 5.0-15467.

Is the issue present in the latest stable version?

No, but the latest stable build crashes in Rosetta 2 when attempting to start a game due to a seemingly different error.

If the issue isn't present in the latest stable version, which is the first broken version?

5.0-14295

What are your PC specifications?

2021 Macbook Pro 16"
M1 Max with 32 GPU Cores

64 GB of RAM
macOS Monterey 12.0.1

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

dolphin.log appears to be empty. I have attached a copy of the crash log that macOS generated.

History

#1 - 11/08/2021 03:59 AM - friendsxix

I am not entirely sure why I specifically called out the ARM64 JIT in the issue title, since it happens with the x86-64 JIT running through Rosetta 2 as well on builds following the introduction of ARM support on Mac.

#2 - 11/08/2021 04:50 AM - OatmealDome

Can't reproduce on an M1.

Seems like mmap in MemArena::CreateView is failing because of an EXC_GUARD exception of type GUARD_TYPE_VIRT_MEMORY. I've never seen such a thing before.

The XNU sources have this to say about that exception type (https://github.com/apple/darwin-xnu/blob/main/osfmk/vm/vm_map.c#L7653): "Right now, we do this when we find nothing mapped, or a gap in the mapping when a user address space deallocate was requested. We report the address of the first gap found."

My specs:
Mac mini (2020)
Apple M1
macOS Monterey 12.0.1

#3 - 11/15/2021 10:03 PM - Rrnd24

I have the same Problem on the latest dev & latest beta.

But it only happens if SIP is disabled or partially disabled.
If SIP is fully enabled (csrutil enable) Dolphin works fine.

#4 - 01/07/2022 04:12 AM - crazyninjadude

Rrnd24 wrote:

> I have the same Problem on the latest dev & latest beta.
>
> But it only happens if SIP is disabled or partially disabled.
> If SIP is fully enabled (csrutil enable) Dolphin works fine.

I had the exact same crashing issue as well. I enabled SIP and it and it fixed the issue as well. Everything runs well enough 5 0-15837 with SIP enabled

Files

dolphincrash.log	41.3 KB	11/08/2021	friendsxix