Cemu - Bug #281

Debugger R/W Breakpoints are Broken

02/26/2020 03:13 AM - potatotomato

Status:	New	**Start date:**	02/26/2020
Priority:	Normal		
Assignee:			
Category:	UI		
API:		**GPU Vendor/Model:**	
Cemu Version:	1.17.2b		

Description

So it seems that read/write breakpoints are broken. As for steps for reproducing the issue, in Breath of the Wild [US v208] with all DLC I found my arrow count using the memory search, which I verified by changing the value and seeing the amount update in-game, and then decided to see what assembly instruction was modifying that amount when I shot an arrow. So using the PPC Debugger, I set a write breakpoint on the address and shot an arrow which then stopped the game's execution at 0x02eb66c0 which is a lwz which is a load word instruction so there is no way that is modifying the arrow count. Also, I stepped forward one instruction and as expected the arrow count stayed the same. Though, I actually do know that the instruction that writes to the arrow count is at 0x02eb6768 so the debugger is stopping at the wrong assembly instruction.

History

#1 - 02/26/2020 09:21 AM - Crementif

In the meantime, you could try using the singlecore-interpreter CPU Mode in the game profile settings. Pretty sure interpreter was the only mode that allowed for stepping previously either so it's a better mode for debugging all around.

#2 - 02/26/2020 06:04 PM - potatotomato

Ah alright. Thanks.

#3 - 02/26/2020 11:21 PM - potatotomato

Okay so it seems to work with the interpreter but it's a little odd because the breakpoint triggers one instruction after the desired instruction.

#4 - 04/10/2021 05:42 PM - Serfrost

Last mention of Breakpoints was 1.22.2

- Fixed memory breakpoints and made them work with our new threading code

However, this may still be broken.