

Forum:[Hack Forums](#)

Thread: [Manual DLL mapping. Crash on load a system DLL.](#)

Securifier - January 14, 2020, 2:23 am

Hello Hackforums.

I'm coding in C++ a manual DLL mapper with a custom GetProcAddress.

I tried to load a DLL I created, and all works fine. I can resolve an exported function, and call it. But when I try with user32.dll to call MessageBoxW, it crashes.

To manual map, I follow these steps :

- Reading file and putting in memory
- Find and check headers
- Allocate memory for mapping DLL (virtual alloc)
- Copy headers and sections
- Fix relocations
- Fix imports
- Call entry point

Even on user32, everything works fine, and I'm able to get a handle that looks valid, i can even find a valid address for my function from GetProcAddress, but when I call it, I get a crash.

Is there something to do in addition on Windows DLL ? It works perfectly on my owns dlls.

Thank you very much :)

SIM-3602340 - January 14, 2020, 3:00 am

Can you provide more info on the crash?

Securifier - January 14, 2020, 3:47 am

HFDone - January 14, 2020, 4:54 am

you get access violation error cuz the dll is in system dir
copy it to your exe path and try it

Securifier - January 15, 2020, 1:58 am

I copied the DLL to my working directory, and i get the same error.

Here a screenshot of the formats of all the executables I use

HFDone - January 15, 2020, 5:19 am

seems you have other problem with your mapping code

also check you are using the right code for your os 32 \ 64 and dll also can be problem using debug option over release ...

Securifier - January 15, 2020, 7:58 am

I just tried with OutputDebugStringA from kernel32, and it works great.....

I don't know why my User32 is broken....

SIM-3602340 - January 15, 2020, 9:51 am

The memory address that visual studio debugger is giving to you is f*d up, like it is supposed to be a valid memory address and obviously it isn't. This means that you are passing a value instead of a pointer somewhere or your relocation is incorrect. That's why we have an access violation error, a function is trying to read memory from that address and it's invalid. Can you dive deeper and show us where the error is occurring? I think that would help

Securifier - January 16, 2020, 3:39 am

The address of my resolved function looks valid: MessageBoxA 0x013C0CD0

LivelyToerag - January 16, 2020, 4:04 am

(Jan 14, 2020 05:54 AM)HFDone Wrote: [\[CITE\]](#) you get access violation error cuz the dll is in system dir

copy it to your exe path and try it

Shut up you don't know what you are talking about.

For the user having problems:

1. Is this for 64 bit or 32?
2. Show the prototype for MessageBoxAPI
3. Show disassembly of where it crashes.
4. Show callstack where it crashes.

If you don't know how to do the last 2 things use Google.

HFDone - January 16, 2020, 4:08 am

(Jan 16, 2020 05:04 AM)LivelyToerag Wrote: [\[CITE\]](#) Shut up you don't know what you are talking about.

For the user having problems:

1. Is this for 64 bit or 32?
2. Show the prototype for MessageBoxAPI
3. Show disassembly of where it crashes.
4. Show callstack where it crashes.

If you don't know how to do the last 2 things use Google.

(Jan 15, 2020 06:19 AM)HFDone Wrote: [\[CITE\]](#) seems you have other problem with your mapping code

also check you are using the right code for your os 32 \ 64 and dll also can be problem using debug option over release ...

LivelyToerag - January 16, 2020, 4:09 am

the way you asked that in the first place shows that you have no reason to be trying to help others when you can't tell the difference between a memory access and opening a file.

skids gonna skid, asking more stupid questions doesn't make you look smart

SIM-3602340 - *January 17, 2020, 6:20 am*

Yes it's definitely very hard to understand what is going on without a detailed crash report. Maybe you should provide the full source to someone, so he can run it and see what's going on..