It rather involved being on the other side of this airtight hatchway: Hanging the loader

devblogs.microsoft.com/oldnewthing/20181219-00

December 19, 2018

Raymond Chen

A security vulnerability report pointed out that a malicious file can cause the module loader to enter an infinite loop, thereby causing a denial of service on the process doing the loading.

This was by itself not interesting. After all, if you have managed to get the system to attempt to load your DLL, and you want to use it to cause a denial of service, then you don't need to get this fancy. You can just put `Sleep(INFINITE);` in your `DLL_ PROCESS_ ATTACH` handler!

In other words, you're already on the other side of the airtight hatchway. And you're bragging that you can do something annoying like a denial service, apparently unaware that being on the other side of the airtight hatchway gives you the ability to do far more interesting (and threatening) things.

Raymond Chen

Follow