Why is my starting directory ignored when I elevate a command prompt?

devblogs.microsoft.com/oldnewthing/20071211-00

December 11, 2007

Raymond Chen

Take a shortcut to the command prompt or some other Windows component, right-click it, and select “Run as Administrator.” The “Start in” directory from the shortcut is ignored and you are always dropped into the system directory. Why is the starting directory ignored? To avoid a category of attacks (current directory attacks). According to the dynamic link library search order documentation, the current directory is searched in step five, after the executable directory, and a variety of system-defined directories. If a program calls `LoadLibrary` and does not pass a fully-qualified path, and the DLL cannot be found in one of the first four locations, the current directory will be searched. An attacker can drop a DLL into a directory and trick you into running a program with that directory as its current directory. When that program tries to load a library that normally doesn’t exist, the one the attacker created will be found and loaded. This is bad.

Note that this behavior applies only to Windows binaries and only if they are launched through an elevation prompt. (Programs that are not a part of Windows do not receive this behavior because compatibility testing showed that third-party application rely heavily on the current directory being preserved across an elevation boundary. For example, installers will unpack their contents into a temporary directory, change to that temporary directory, and then run the main setup program.)

Raymond Chen

Follow