**Dll Spoofing**

**Note:** DLL spoofing is not always considered as a denial of service attack. In this document we describe a specific form of DLL spoofing that causes denial of service.

**Description**

If an attacker gains control of one of the directories on the DLL search path, it can place a malicious copy of the DLL in that directory. This is sometimes called a DLL preloading attack or a binary planting attack. If the system does not find a legitimate copy of the DLL before it searches the compromised directory, it loads the malicious DLL and therefore it cannot load the dll it depends on. **[1]** an intruder can spoof dlls tocompromise a process.

**Reference**

**[1]** <https://msdn.microsoft.com/en-us/library/ff919712(VS.85).aspx>