Presonus Studio One 6

Vulnerability Summary

- **Title:** DLL Search Order Hijacking in Presonus Studio One 6
- **Summary:** A DLL Search Order Hijacking vulnerability was identified in the executable Presonus Studio One 6 (Studio One.exe) in version 6.6.1.99821. The software searches for DLLs in an insecure order, allowing an attacker to hijack the search process and load a malicious DLL, leading to potential code execution and system compromise.

Vulnerability Details

- **Description:** Presonus Studio One 6 improperly handles the search order for loading DLLs, resulting in a vulnerability known as DLL Search Order Hijacking. This issue occurs because the software includes directories that are user-controllable or writable in the search path before system directories. An attacker can place a malicious DLL in one of these directories, which will be loaded by the software instead of the legitimate DLL.
- **Impact:** Successful exploitation can lead to arbitrary code execution with the same privileges as the running process. This can result in privilege escalation, data theft, system compromise, and further exploitation.
- **Attack Vector:** Local
- **Attack Complexity:** Low
- **Privileges Required:** Low
- **User Interaction:** Required

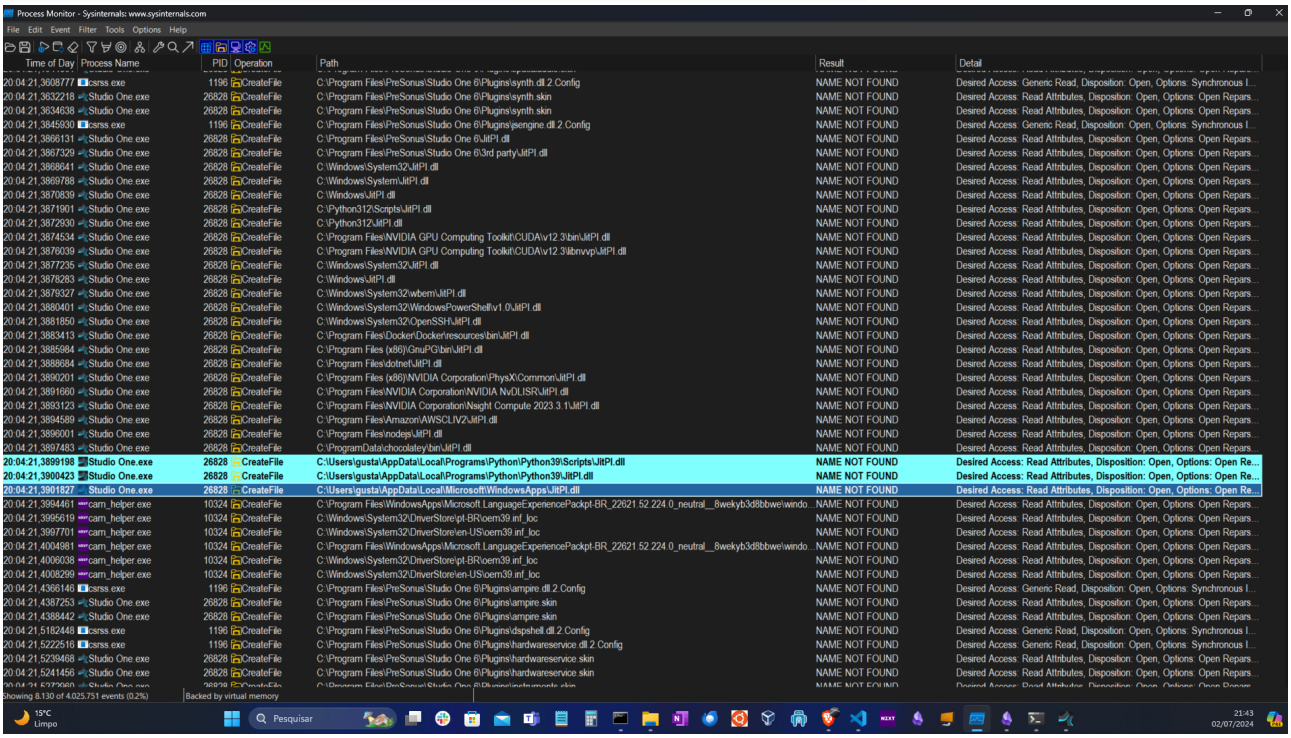
Affected Products

- **Product Name:** Presonus Studio One 6
- **Version(s):** 6.6.1.99821

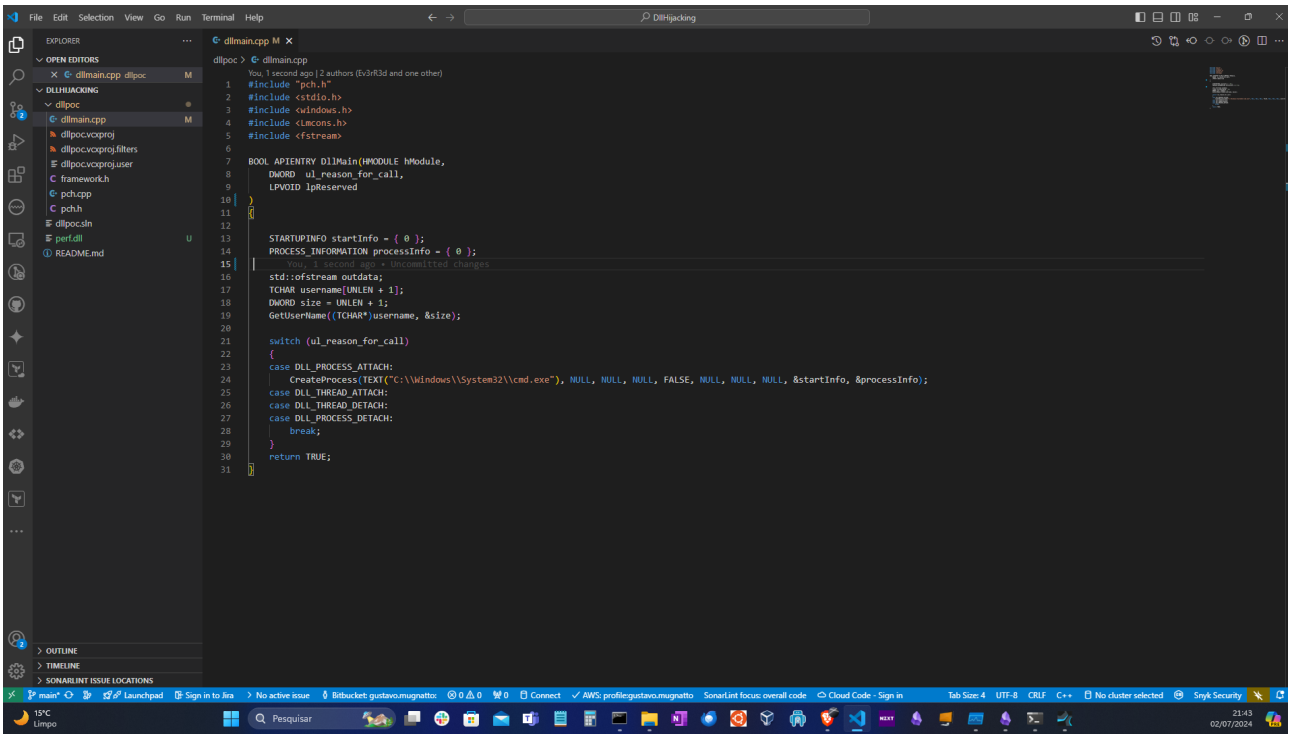
Steps to Reproduce

1. Install Presonus Studio One 6 version 6.6.1.99821 on a target machine.

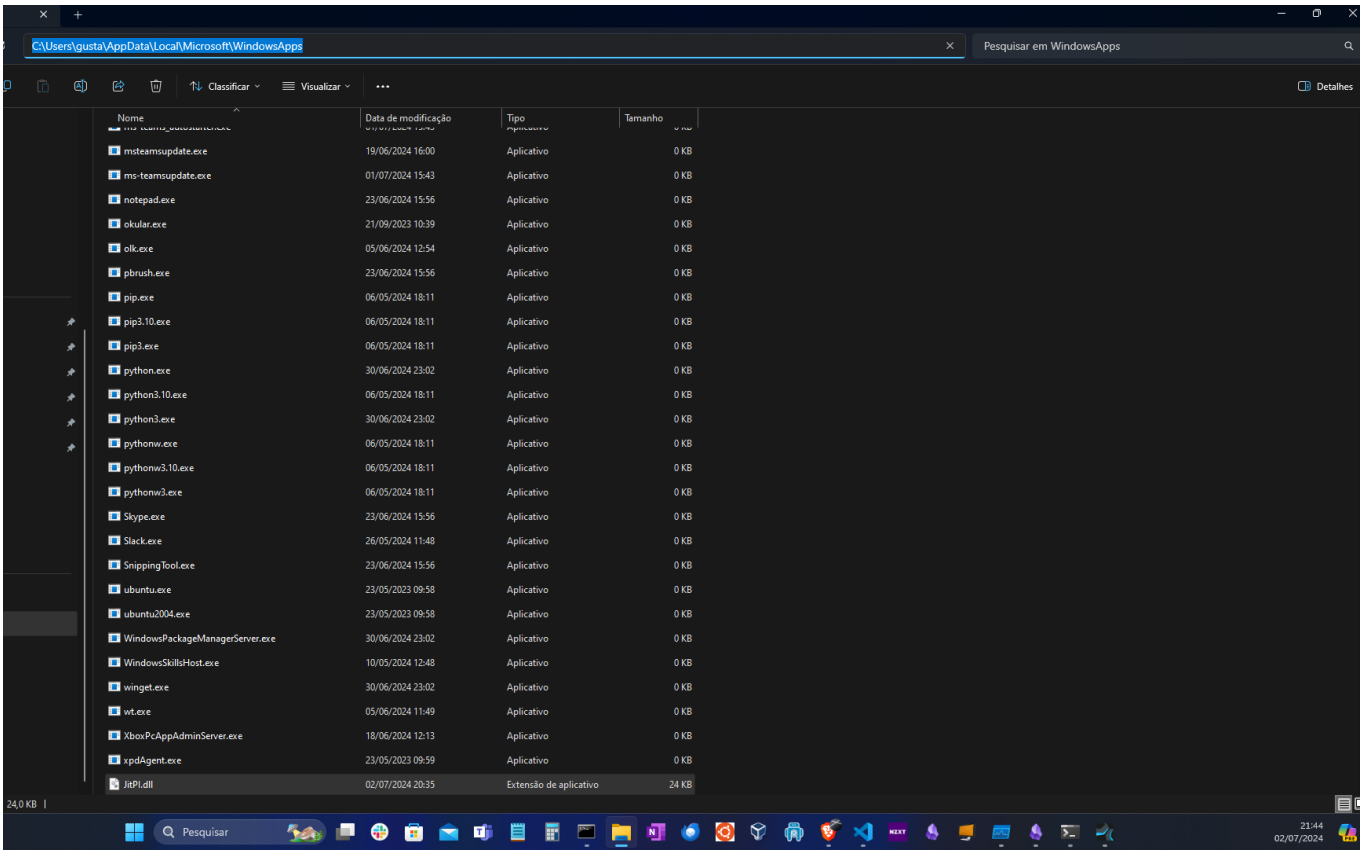
2. Identify a DLL that the software loads during execution using Procmon64. The executable looks for a DLL under `C:\Users\<user>\AppData\Local\Microsoft\WindowsApps\JitPI.dll`



3. Create a malicous DLL and rename as the same DLL that the software is looking for.



4. Place a malicious DLL with the same name as the legitimate DLL in a directory that is searched before the legitimate directory (e.g., the current working directory or a directory specified in the PATH environment variable).



5. Execute Studio One 6 and the malicious DLL is loaded. A cmd.exe opens in the background. If the executable is runnig as Administrator, the cmd.exe runs as admin.