**Abstract**

In the following thesis we examine how Event Tracing for Windows and function hooking can be used to detect exploitation of a recently patched vulnerability in Windows. To do so we analyze how Event Tracing and function hooking works in Windows, and how it can be used to detect exploitation attempts of known vulnerabilities. We do so by analyzing the root cause of CVE-2021-24086 in order to create a fully functional Proof of Concept. Using this Proof of Concept we detect an exploitation attempt of CVE-2021-24086 on a Windows 10 system. We do so by simulating function hooking using a debugger, to showcase the flexibility and extensibility of function hooking. Furthermore, we also explore how Microsoft uses Event Tracing for Windows to generate events for unintended states and explain why this cannot be used to detect vulnerability exploitation attempts. Finally, we analyze and discuss how the process of creating exploitation detection for CVE-2021-24086 can be scaled and automated to detect exploitation attempts of other recently patched vulnerabilities given patch information.