Investigating CVE-2022-1729: Linux Kernel Perf Subsystem Vulnerability

Sahil Upasane (22BPS1059), Souradeep Dutta (22BPS1053)

Abstract

This project focuses on studying and resolving CVE-2022-1729, a significant vulnerability found in the Linux kernel's perf subsystem. Rated as high-risk with a CVSS score of 7.0, this vulnerability stems from a use-after-free issue in the kernel's performance events feature. A related concern is a race condition within `perf_event_open()`, which could be exploited by an unauthorized user to gain root privileges. This flaw creates possibilities for different types of attacks, such as leaking kernel address information and executing arbitrary code.

The main goals of this study are:

1. **Understanding the Vulnerability:** Thoroughly comprehending the use-after-free problem, its connection to race conditions, and potential consequences.
2. **Linux Perf Subsystem Overview:** Gaining insight into the purpose and functioning of the Linux perf subsystem, known for profiling and tracing capabilities.
3. **Local Privilege Escalation:** Investigating how the vulnerability allows unauthorized users to escalate their privileges, resulting in unauthorized system access.
4. **Affected Kernel Versions:** Identifying the range of Linux kernel versions that are vulnerable to this issue and providing historical context.
5. **Mitigating the Impact:** Exploring strategies to minimize the vulnerability's impact on system security and functionality.

This project aims to establish a foundational understanding of CVE-2022-1729 and its implications in the Linux kernel's perf subsystem. This understanding will guide subsequent phases, where potential solutions and security measures will be explored further. Our approach involves closely analyzing the vulnerability's behavior, studying source code, conducting controlled testing, and evaluating affected kernel versions. We will also explore possible ways to mitigate the issue, propose a theoretical patch, assess its impact on system performance, and thoroughly document our findings. While this phase focuses on theoretical investigation, it lays the groundwork for practical implementation and testing to effectively address the vulnerability.