Severity

High

Analysis Summary

CVE-2022-21499 CVSS:9.1

Linux Kernel could allow a remote attacker to bypass security restrictions, caused by a lockdown break issue. By sending a specially-crafted request using the kernel debugger, an attacker could exploit this vulnerability to perform read and write access to kernel memory.

CVE-2022-1786 CVSS:7.8

Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by an invalid-free flaw in the io_uring subsystem. By executing a specially-crafted program, an authenticated attacker could exploit this vulnerability to gain elevated privileges or cause a denial of service condition.

Impact

- Security Bypass
- Privilege Escalation

Indicators Of Compromise

CVE

- CVE-2022-21499
- CVE-2022-1786

Affected Vendors

- Linux

Affected Products

- Linux Kernel
- Linux Kernel 5.10

Remediation

Refer to Linux Kernel GIT Repository for patch, upgrade or suggested workaround information.

CVE-2022-21499 CVE-2022-1786