Severity

High

Analysis Summary

CVE-2022-1652

Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

Impact

- Code Execution

Indicators Of Compromise

CVE

CVE-2022-1652

Affected Vendors

Linux

Affected Products

Linux Kernel 5.17.5

Remediation

Upgrade to the latest version of Linux, available from the Linux Kernel WebSite.

Linux Kernel Web site