Severity

Medium

Analysis Summary

CVE-2022-1419

Linux Kernel could allow a local authenticated attacker to execute arbitrary code on the system, caused by a use-after-free flaw in the update 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-2022-1419

Affected Vendors

Linux

Affected Products

- Linux Kernel 4.19

Remediation

Refer to Linux Kernal Website for patch, upgrade, or suggested workaround information.

Linux Kernel Website