Severity

High

Analysis Summary

CVE-2022-28893

Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a use-after-free flaw in the inet_put_port function in the SUNRPC subsystem. By sending a specially-crafted request, 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-2022-28893

Affected Vendors

Linux

Affected Products

Linux Kernel 5.17.2

Remediation

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

Linux Kernel GIT Repository