Severity

High

Analysis Summary

CVE-2022-29800, CVSS: 7

Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a TOCTOU race condition flaw in the networkd-dispatcher daemon in the systed component. By sending a specially-crafted request using a rogue D-Bus service, an authenticated attacker could exploit this vulnerability to execute arbitrary code with root privileges.

CVE-2022-29799, CVSS: 7.8

Linux Kernel could allow a local authenticated attacker to traverse directories on the system, caused by not sanitize the OperationalState or the AdministrativeState in the networkd-dispatcher daemon in the systemd component. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to write arbitrary files on the system.

Impact

- Privilege Escalation
- File Encryption
- Obtain Information

Indicators Of Compromise

CVE

- CVE-2022-29800
- CVE-2022-29799

Affected Vendors

- Linux

Affected Products

- Linux Kernel

Remediation

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

CVE-2022-29800

CVE-2022-29799