مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Privilege Escalation Vulnerability in LINUX

Tracking #:432317457

Date:07-07-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical local privilege escalation vulnerability (**CVE-2025-6019**) that affects Linux systems using udisksd and libblockdev, allowing users in the allow_active group to gain root access. A proof-of-concept is publicly available, and exploitation is trivial in misconfigured environments.

## TECHNICAL DETAILS:

**Vulnerability Details:**

- **CVE-2025-6019**
  - **CVSS 3.x Base Score:** 7.0 (HIGH)
  - **Affected Components:** udisksd, libblockdev, D-Bus, Polkit
  - **Affected Distributions:**
    - Fedora 40+
    - SUSE Linux (with udisks2 and libblockdev)
    - Any Linux system using allow_active group for disk permissions
  - **Root Cause:**
    - Improper trust in group membership (allow_active) for privileged disk operations via D-Bus.
    - Weak Polkit/D-Bus validation rules allow unauthorized mounting and volume operations.
  - **Exploit Conditions:**
    - udisksd is installed and running.
    - A user is in the allow_active group.
    - Polkit rules are default or misconfigured.
  - **Proof-of-Concept:**
    - Exploit demonstrated using Python scripts or D-Bus CLI to trigger root-level disk mounts.
    - Potential for full root compromise when chained with volume management APIs.
  - **Patch Status:**
    - Logic updated to enforce root-only disk operations.
    - Polkit rules hardened for /org/freedesktop/UDisks2/Manager.

## RECOMMENDATIONS:

- **Update Immediately:** Apply latest patches for udisks2 and libblockdev.
- **Audit Group Membership:** Review and restrict users in the allow_active group.
- **Harden Polkit Policies:** Tighten rules for disk and volume operations.
- **Limit Exposure:** Avoid running udisksd on multi-user systems without sandboxing or containerization.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:


- https://nvd.nist.gov/vuln/detail/CVE-2025-6019