مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Red Hat Udisks Daemon

Tracking #:432317657

Date:01-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity flaw in the Red Hat Udisks daemon, a component that provides a D-BUS interface for managing storage devices on Linux systems. The vulnerability allows unprivileged local users to exploit an out-of-bounds read issue, potentially accessing files owned by privileged accounts or causing a daemon crash.

TECHNICAL DETAILS:

Red Hat has disclosed a critical security flaw in the Udisks daemon, which provides a D-BUS interface for managing storage devices such as loop devices. The vulnerability, tracked as CVE-2025-8067, allows unprivileged local users to exploit an out-of-bounds read condition, potentially leading to disclosure of sensitive information or a denial of service (DoS).

Vulnerability Details

- CVE-2025-8067
- CVSS Score 8.5 High
- The Udisks daemon fails to properly validate that the file index parameter is non-negative in loop device management, enabling negative indices to cause memory read outside of the intended bounds. This may result in the exposure of sensitive memory, including cryptographic materials, or process crashes leading to denial of service.

Affected Products

- **Red Hat Enterprise Linux (RHEL):**
  - RHEL 6 (udisks) – (No patches due to EOL)
  - RHEL 7, 8, 9, 10 (udisks2)

Remediation

- Install the updated Udisks packages

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Red Hat.

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://access.redhat.com/security/cve/CVE-2025-8067