

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Local Privilege Escalation Vulnerability in RefluXFS Linux Kernel
Tracking #:432319330
Date:24-07-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical local privilege escalation vulnerability, CVE-2026-64600, dubbed RefluXFS, has been disclosed in the Linux kernel's XFS filesystem implementation.

TECHNICAL DETAILS:

A critical local privilege escalation vulnerability, CVE-2026-64600, dubbed RefluXFS, has been disclosed in the Linux kernel's XFS filesystem implementation. The flaw affects systems using reflink-enabled XFS filesystems and allows an unprivileged local attacker to gain root privileges by exploiting a race condition in the XFS copy-on-write (CoW) mechanism.

The vulnerability has reportedly existed since Linux kernel 4.11 and impacts multiple enterprise Linux distributions, including RHEL, Oracle Linux, Rocky Linux, AlmaLinux, Amazon Linux, Fedora, CentOS Stream, and potentially Debian, Ubuntu, and SUSE systems configured with reflink-enabled XFS. Due to the potential for persistent filesystem modification and privilege escalation, organizations should prioritize patching affected systems and rebooting into updated kernels.

Vulnerability Details

- CVE ID: CVE-2026-64600
- Vulnerability Name: RefluXFS
- Severity: Critical
- Affected Component: Linux Kernel XFS Filesystem (Copy-on-Write/Reflink)
- Attack Vector: Local
- Privileges Required: Low (Unprivileged Local User)
- User Interaction: None
- The vulnerability is caused by a race condition in the XFS copy-on-write (CoW) implementation.
- During concurrent direct I/O operations on reflink-enabled files, XFS temporarily releases an inode lock while waiting for transaction log space.
- An attacker can exploit this timing window by modifying block mappings before the original write resumes.
- The resumed operation incorrectly assumes the filesystem block is private and performs writes directly to shared blocks.
- This results in arbitrary on-disk block overwrites affecting legitimate files.

Affected Systems:

The vulnerability affects systems meeting all of the following conditions:

- Running Linux Kernel 4.11 or later (prior to vendor patches).
- Using an XFS filesystem.
- Reflink support enabled on the XFS filesystem.
- Local users have write access to at least one directory on the affected filesystem.

Confirmed Affected Distributions

- Red Hat Enterprise Linux (RHEL) 8
- Red Hat Enterprise Linux (RHEL) 9
- Red Hat Enterprise Linux (RHEL) 10
- CentOS Stream

- Oracle Linux
- Rocky Linux
- AlmaLinux
- CloudLinux
- Amazon Linux
- Fedora Server 31 and later

Potentially Affected

- Debian
- Ubuntu
- SUSE Linux

(If XFS with reflink support is configured.)

RECOMMENDATIONS:

Immediate Actions:

- Inventory all Linux systems using XFS filesystems.
- Identify systems with reflink-enabled XFS volumes.
- Prioritize:
 - Internet-facing Linux servers.
 - Multi-user systems.
 - Shared hosting environments.
 - Multi-tenant infrastructure.
- Apply vendor-provided Linux kernel security updates immediately.
- Perform a full system reboot after patch installation to activate the updated kernel.
- Restrict local shell access to trusted users wherever possible.

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://blog.qualys.com/vulnerabilities-threat-research/2026/07/22/refluxfs-a-linux-kernel-local-privilege-escalation-to-root-in-xfs-cve-2026-64600>