# Two-Year-Old Linux OverlayFS Privilege Escalation Vulnerability Exploited

**TL;DR**

*Attackers are actively exploiting CVE-2023-0386, a high-severity vulnerability in the Linux kernel's OverlayFS subsystem, to escalate privileges from local user accounts directly to root.*

*Exploitation involves abusing filesystem permissions to place malicious setuid binaries in writable locations, granting attackers complete administrative control. Organizations must patch immediately or temporarily disable OverlayFS to prevent compromise.*

## Overview

CISA recently added CVE-2023-0386 (CVSS 7.8) to its Known Exploited Vulnerabilities (KEV) catalog after confirming active exploitation. The flaw is two years old and affects the Linux kernel's OverlayFS subsystem. CVE-2023-0386 allows a local user to escalate privileges by improperly handling file ownership permissions when copying capable files between different mount points.

The vulnerability stems from improper validation in the Linux kernel's OverlayFS when files with special permissions (setuid binaries) are copied from a nosuid mount to another filesystem. Attackers exploit this oversight to create a root-owned executable within writable locations, typically in directories such as /tmp. Execution of this binary grants instant administrative privileges, significantly compromising security, especially in containerized and multi-tenant environments that extensively use OverlayFS.

### Affected Products

- Linux kernel versions prior to commit 4f11ada10d0a
- Red Hat Enterprise Linux (RHEL) versions 7, 8, and 9
- Ubuntu and Debian distributions with unpatched OverlayFS implementations
- NetApp ONTAP Select and SolidFire products

Attackers rely on organizations overlooking older kernel vulnerabilities, especially those exploitable locally. While federal agencies have until July 8, 2025, to patch CVE-2023-0386 per CISA guidelines, Aspire strongly advises immediate patching to avoid potential compromise.

## Aspire Protects

- **Patch** – Immediately apply vendor-provided Linux kernel patches addressing CVE-2023-0386. You can find the official Linux kernel patch in this GitHub repository. Further details can be found here.
- Temporarily disable or restrict OverlayFS functionality if patches cannot be immediately applied.
- Monitor for suspicious setuid binaries appearing in writable directories like /tmp or container layers.
- Limit user privileges and audit user activity on shared systems or containers until patched.

### TTPs to Watch

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.003] – Attackers abuse OverlayFS to manipulate setuid binaries for privilege escalation.

Defense Evasion

- Exploitation for Privilege Escalation [T1068] – Exploiting kernel-level vulnerabilities allows attackers to circumvent standard filesystem restrictions.

### IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

### Targeted Industries

Organizations within these sectors using vulnerable Linux kernel versions and containerized environments are particularly vulnerable:

- Education
- Healthcare
- Retail and eCommerce
- Government
- Finance
- Cloud Service Providers

- Information Technology
- Telecommunications

## Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

## Supporting Documentation

CVE Record: CVE-2023-0386

Known Exploited Vulnerabilities Catalog | CISA

CVE-2023-0386 - Red Hat Customer Portal

ovl: fail on invalid uid/gid mapping at copy up - kernel/git/torvalds/linux.git - Linux kernel source tree