Dirty Frag Linux Kernel Local Privilege Escalation Vulnerability

TL;DR

There is a new Linux kernel local privilege escalation vulnerability class known as "Dirty Frag." The issue affects networking-related Linux kernel components and allows a local unprivileged user to gain root privileges on vulnerable systems.

The vulnerability impacts multiple Linux kernel versions across major distributions. There is currently no CVE assigned and no official patch available.

Overview

There is a Linux kernel privilege escalation vulnerability class known as "Dirty Frag." According to reporting, the issue affects the xfrm-ESP and RxRPC subsystems and stems from improper handling of page cache operations inside the Linux kernel.

The vulnerability allows a local unprivileged user to modify protected files in memory and gain root privileges on the affected system. The affected code paths date back to 2017 and impact multiple Linux kernel versions across major distributions.

Although exploitation requires local access, the vulnerability still creates risk for shared systems, development environments, and Linux systems already compromised through malware or stolen credentials. Once root access is obtained, a threat actor can take full control of the affected system.

Currently, there are no official patches or CVE identifiers available. Aspire recommends monitoring Linux vendor advisories closely and applying patches as soon as they become available.

Aspire Protects

- Monitor Linux vendor advisories for patches and updated kernel packages.
- Restrict unnecessary local access to Linux systems.
- Review privileged account and sudo access.
- Monitor systems for unusual privilege escalation activity.
- Prioritize patching internet-facing Linux systems once fixes become available.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit vulnerable Linux kernel functionality to gain root privileges on the affected system.

IoCs

There are no known IoCs 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

The Dirty Frag vulnerability threatens organizations running Linux-based servers, appliances, virtual machines, cloud workloads, or development environments.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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

Advisory: Linux Kernel LPE - Dirty Frag