master Go to file Code

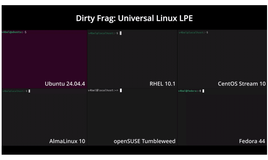
V4bel template 07995be · 11 hours ago

| | | |
|---|---|---|
| assets | CVE | 11 hours ago |
| README.md | template | 11 hours ago |
| exp.c | typo | yesterday |

README

# Dirty Frag: Universal Linux LPE


## Abstract




This document describes the Dirty Frag vulnerability class, first discovered and reported by Hyunwoo Kim (@v4bel), which can obtain root privileges on major Linux distributions by chaining the `xfrm-ESP Page-Cache Write` vulnerability and the `RxRPC Page-Cache Write` vulnerability.

Dirty Frag is a case that extends the bug class to which Dirty Pipe and Copy Fail belong. Because it is a deterministic logic bug that does not depend on a timing window, no race condition is required, the kernel does not panic when the exploit fails, and the success rate is very high.

For detailed technical information and the timeline, see here.

Because the embargo has currently been broken, no patch or CVE exists. After consultation with the maintainers on linux-distros@vs.openwall.org and at their request, this Dirty Frag document is being published. For the disclosure timeline, refer to the technical details.

> Note
>
> **2026-05-08 Update:**
>
> - The `xfrm-ESP Page-Cache Write` vulnerability has been assigned `CVE-2026-43284` and patched in mainline at f4c50a4034e6.
> - The `RxRPC Page-Cache Write` vulnerability has been reserved as `CVE-2026-43500` for tracking; no patch exists in any tree yet.

## Exploiting

### One-line special

```
git clone https://github.com/V4bel/dirtyfrag.git
```

This PoC is provided as accurate information following consultation with linux-distros. Do not use it on systems that you are not authorized to test.

### Cleanup

⚠️ **Important:** After running this exploit, the page cache is contaminated. To clear the polluted page cache and ensure system stability, either run:

```
echo 3 > /proc/sys/vm/drop_caches
```

or reboot the system.

## Affected Versions

The xfrm-ESP Page-Cache Write vulnerability is in scope from cac2661c53f3 (2017-01-17) up to upstream, and the RxRPC Page-Cache Write vulnerability is in scope from 2dc334f1a63a (2023-06) up to upstream.

In other words, the effective lifetime of the vulnerabilities is about 9 years.

This Dirty Frag has been tested on the following distribution versions.

- Ubuntu 24.04.4: 6.17.0-23-generic
- RHEL 10.1: 6.12.0-124.49.1.el10_1.x86_64
- openSUSE Tumbleweed: 7.0.2-1-default
- CentOS Stream 10: 6.12.0-224.el10.x86_64
- AlmaLinux 10: 6.12.0-124.52.3.el10_1.x86_64
- Fedora 44: 6.19.14-300.fc44.x86_64
- ...

## Mitigation

1. Because the responsible disclosure schedule and the embargo have been broken, no patch exists for any distribution. Use the following command to remove the modules in which the vulnerabilities occur and clear the page cache.

```
sh -c "printf 'install esp4 /bin/false\ninstall r
```

2. Once each distribution backports a patch, update accordingly.

## FAQ

### Why did you chain two vulnerabilities?

xfrm-ESP Page-Cache Write provides a powerful arbitrary 4-byte STORE primitive like Copy Fail, and is included on most distributions, but it requires the privilege to create a namespace.

Ubuntu sometimes blocks unprivileged user namespace creation through AppArmor policy. In such an environment, xfrm-ESP Page-Cache Write cannot be triggered. RxRPC Page-Cache Write does not require the privilege to create a namespace, but the `rxrpc.ko` module itself is not included in most distributions. However, on Ubuntu, the `rxrpc.ko` module is loaded by default.

Chaining the two variants makes the blind spots cover each other, allowing root privileges to be obtained on every major distribution. For details, refer to the technical details document.

### Another "branded" "Dirty" series?

Yeah, yeah, I know. However, this vulnerability is a descendant of "Dirty Pipe", and it is a bug class that "dirties" the `frag` member of `struct sk_buff`, so this name is the most appropriate.

## About

*No description, website, or topics provided.*

Readme
Activity
2.7k stars
34 watching
420 forks
Report repository

## Releases

No releases published

## Packages

No packages published

## Contributors 2

V4bel V4bel
Nriver Nate River

## Languages

C 100.0%

## What is its relationship with the "Copy Fail" vulnerability?

Copy Fail was the motivation for starting this research. In particular, xfrm-ESP Page-Cache Write in the Dirty Frag vulnerability chain shares the same sink as Copy Fail. However, it is triggered regardless of whether the algif_aead module is available. In other words, even on systems where the publicly known Copy Fail mitigation (algif_aead blacklist) is applied, your Linux is still vulnerable to Dirty Frag.

## So, how do I fix my Linux?

Refer to the Mitigation and Disclosure Timeline sections. Due to external factors, the embargo has been broken, so no patch exists for any distribution.