Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Three Strikes in Two Weeks: Fragnesia Joins the Dirty Frag Family

Date of Publication	Admiralty Code	TA Number
May 19, 2026	A1	TA2026136

Summary

First Seen: May 13, 2026
Affected Products: Linux Kernel (XFRM ESP-in-TCP subsystem) across AlmaLinux 8/9/10 and AlmaLinux Kitten 10, Amazon Linux, CloudLinux, Debian, Fedora, Gentoo, openSUSE, Red Hat Enterprise Linux, SUSE, Ubuntu, and OpenShift.
Impact: Fragnesia (CVE-2026-46300) poses an immediate and severe risk to multi-tenant Linux environments, container clusters, CI/CD runners, build farms, cloud SaaS platforms running user code, and any host where untrusted users can obtain a local shell. Crucially, unlike its Dirty Frag predecessor, Fragnesia requires no host-level privileges, expanding the population of attackers who can weaponize it after any initial foothold, such as a compromised SSH account, web shell, container escape, or low-privileged service account. The deterministic, non-race-condition nature of the primitive substantially lowers the operational bar for reliable root escalation across vulnerable kernels, magnifying the post-compromise blast radius of even minor initial intrusions.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-46300	Fragnesia (Linux Kernel XFRM ESP-in-TCP Page-Cache Corruption Local Privilege Escalation Vulnerability)	Linux Kernel (XFRM ESP-in-TCP / `skb_try_coalesce()` `SKBFL_SHARED_FRAG` propagation)	✗	✗	✓

Vulnerability Details

#1

Fragnesia (CVE-2026-46300), a new local privilege escalation (LPE) vulnerability in the Linux kernel's XFRM ESP-in-TCP subsystem and the third local-root flaw to surface in the same code area within two weeks, following **Copy Fail (CVE-2026-31431)** and the **Dirty Frag pair (CVE-2026-43284 and CVE-2026-43500)**. Fragnesia is a logic flaw in the Linux kernel's socket-buffer fragment handling, classified within the same "Dirty Frag" family as CVE-2026-43284, CVE-2026-43500, and the earlier Copy Fail (CVE-2026-31431) page-cache corruption issues. The defect was introduced as an unintended side effect of an upstream patch shipped to address CVE-2026-43284, and was disclosed publicly on May 13, 2026.

#2

At its root, the bug lies in `skb_try_coalesce()`, which fails to propagate the `SKBFL_SHARED_FRAG` flag when paged fragments are transferred between socket buffers. As a result, the kernel loses metadata indicating that a fragment is externally backed, for example, by page-cache pages spliced into the buffer from a file on disk. The XFRM ESP-in-TCP receive path subsequently performs in-place AES-GCM decryption directly over these page-cache pages, allowing an unprivileged process to XOR a chosen keystream into the cached contents of read-only files.

#3

The vulnerable code paths sit in the `esp4`, `esp6`, and `rxrpc` kernel modules. All supported AlmaLinux releases (8, 9, 10) are affected through `esp4`/`esp6`, with AlmaLinux 9 and 10 additionally exposed via `rxrpc` only on hosts that install the `kernel-modules-partner` package; AlmaLinux 8 does not build `rxrpc`. Advisories have also been published by Amazon Linux, CloudLinux, Debian, Gentoo, Red Hat Enterprise Linux, SUSE, and Ubuntu, confirming impact across essentially every major distribution. Wiz researchers note that AppArmor restrictions on unprivileged user namespaces, such as those enabled by default on Ubuntu, may serve as a partial mitigation, though additional bypass primitives would be required for successful exploitation in those environments. Unlike Dirty Frag, no host-level privileges are required.

#4

DirtyDecrypt, also known as DirtyCBC, is a variant of CopyFail, DirtyFrag, and Fragnesia. A recently patched local privilege escalation vulnerability in the Linux kernel's rxgk module now has a proof-of-concept exploit that allows attackers to gain root access on some Linux systems. While there is no official CVE ID associated with this security flaw. Linux users on distros potentially affected by DirtyDecrypt are advised to install the latest kernel updates as soon as possible.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-46300	Linux Kernel (XFRM ESP-in-TCP / `esp4`, `esp6`, `rxrpc` modules) – impacts AlmaLinux 8/9/10, AlmaLinux Kitten 10, Amazon Linux, CloudLinux, Debian, Fedora, Gentoo, openSUSE, Red Hat Enterprise Linux, SUSE, Ubuntu, and OpenShift	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	CWE-123

Recommendations

Apply Vendor Kernel Patches Immediately: Install the patched kernel released by your Linux distribution as soon as it is available and reboot to load the new kernel. AlmaLinux has shipped patched builds in its testing repository (`kernel-4.18.0-553.124.3.el8_10`, `kernel-5.14.0-611.54.5.el9_7`, `kernel-6.12.0-124.56.3.el10_1`) with production rollout to follow, and advisories with patches or assessments have been published by Amazon Linux, CloudLinux, Debian, Gentoo, Red Hat Enterprise Linux, SUSE, and Ubuntu. Because a public proof-of-concept exists and the exploitation primitive is deterministic, patch deployment should be treated as urgent, particularly for multi-tenant hosts, container clusters, CI runners, and build farms.

Interim mitigation where immediate patching is not feasible: For systems that cannot be rebooted or updated inside the patch window (change freezes, regulated environments, kernel-locked appliances, or third-party driver dependencies), apply the same module-blocklisting workaround used for Dirty Frag. This neutralizes the vulnerable code paths shared across the DirtyDecrypt, Dirty Frag, and Fragnesia cluster by preventing the esp4, esp6, and rxrpc modules from loading and by flushing the page cache to clear any pre-existing poisoned entries:
sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' > /etc/modprobe.d/dirtyfrag.conf; rmmod esp4 esp6 rxrpc 2>/dev/null; echo 3 > /proc/sys/vm/drop_caches; true"

Blacklist or Unload the Vulnerable Modules Until Patched: Where the patched kernel cannot yet be installed, neutralize the attack surface by preventing the `esp4`, `esp6`, and `rxrpc` modules from loading. This is the same mitigation applied for Dirty Frag and addresses Fragnesia identically. Administrators can write a `modprobe` configuration that forces these modules to `/bin/false` and unload any active instances, which is safe on workloads that do not use IPsec transport mode or AFS/rxrpc. Systems already protected against Dirty Frag through this method require no further mitigation action for Fragnesia.

Drop the Page Cache After Mitigation if Compromise is Suspected: Because the Fragnesia exploit corrupts page-cache pages of sensitive files such as `/usr/bin/su` and potentially `/etc/passwd` without altering the on-disk binaries, applying module blacklisting alone is insufficient on hosts that may have been targeted before mitigation. Executing `echo 3 > /proc/sys/vm/drop_caches` evicts cached pages so subsequent reads pull fresh content from disk, removing any in-memory tampering. This operation is safe to run on live systems and is recommended after mitigation on any host with unexplained activity or shared-tenancy exposure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.006: Vulnerabilities
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Defense Evasion	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1611: Escape to Host	
Initial Access	T1078: Valid Accounts	
Credential Access	T1003: OS Credential Dumping	

Patch Links

https://almalinux.org/blog/2026-05-13-fragnesia-cve-2026-46300/

https://access.redhat.com/security/cve/CVE-2026-46300

https://access.redhat.com/security/vulnerabilities/RHSB-2026-003

https://ubuntu.com/security/CVE-2026-46300

https://www.suse.com/security/cve/CVE-2026-46300.html

https://security-tracker.debian.org/tracker/CVE-2026-46300

https://aws.amazon.com/security/security-bulletins/rss/2026-029-aws/

https://blog.cloudlinux.com/fragnesia-mitigation-and-kernel-update

https://bugs.gentoo.org/show_bug.cgi?id=CVE-2026-46300

https://lists.openwall.net/netdev/2026/05/13/79

https://lore.kernel.org/all/agVpIsaSherjHTYg@sultan-box/

https://lore.kernel.org/all/agW4vC0r8QOUKtRT@v4bel/

References

https://www.wiz.io/blog/fragnesia-linux-kernel-local-privilege-escalation-via-esp-in-tcp

https://www.microsoft.com/en-us/security/blog/2026/05/08/active-attack-dirty-frag-linux-vulnerability-expands-post-compromise-risk/

https://github.com/v12-security/pocs/tree/main/fragnesia

https://github.com/v12-security/pocs/tree/main/dirtydecrypt

https://hivepro.com/threat-advisory/dirty-frag-a-2017-optimization-that-aged-into-a-root-exploit/

https://hivepro.com/threat-advisory/one-script-every-distro-full-root-copy-fail-vulnerability-rewriting-linux-threat-models/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 19, 2026 • 04:00 AM

More at www.hivepro.com