I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Escalada de privilegios / Ejecución local de código
Nivel de riesgo: Alta

II. ALERTA

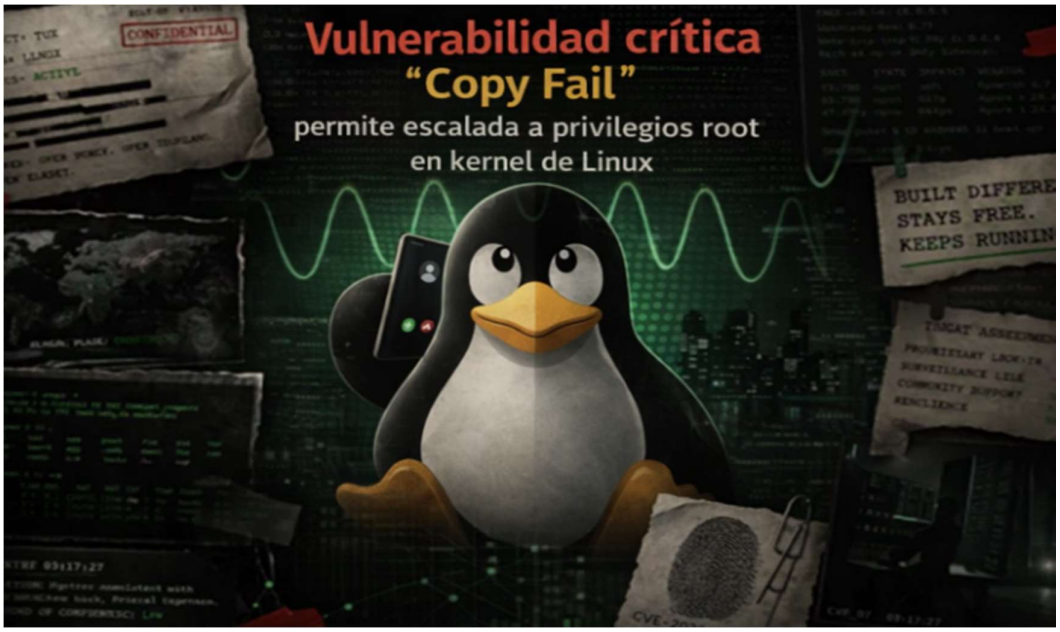

Figura 1.- Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux - figura referencial

Se ha revelado una nueva vulnerabilidad del kernel de Linux denominada "Copy Fail" y registrada como CVE-2026-31431. Esta falla permite a un usuario local sin privilegios escribir 4 bytes en la page cache del kernel de cualquier archivo que sea legible y conseguir acceso ROOT. Afecta a las principales distribuciones de Linux lanzadas desde 2017, incluyendo a Ubuntu, RHEL, SUSE y Amazon Linux, así también como entornos WSL2 y plataformas de contenedores dockers.

III. INTRODUCCIÓN

CVE-2026-31431 fue descubierta por el investigador Theori Taeyang Lee, mientras estudiaba cómo el subsistema criptográfico de Linux interactúa con los datos respaldados por la page cache (es un mecanismo del Linux kernel que guarda en la memoria

RAM copias de archivos que están en disco, para acceder a ellos más rápido) Asistido por IA, Theori, utilizo Xint Code para escalar su investigación en todo el subsistema criptográfico llevando al hallazgo de Copy Fail. Posteriormente investigadores de Xint Code Research Team desarrollaron un PoC (prueba de concepto), incluyendo un exploit en Python de aproximadamente 732 bytes, que aprovechaba este fallo lógico en el módulo authenc, que es parte de ese subsistema criptográfico del Linux kernel.

El exploit abusa de la interacción entre la interfaz de socket AF_ALG y la llamada al sistema splice(), aquí el atacante puede realizar una escritura controlada de 4 bytes en la page cache del kernel de cualquier archivo legible o que tenga permisos de lectura. Esto permite corromper las representaciones en memoria de binarios privilegiados (por ejemplo, /usr/bin/su) sin modificar el archivo en disco.

El PoC público ha sido probado con éxito en kernel utilizados en entornos como Ubuntu, Amazon Linux, Red Hat Enterprise Linux y SUSE Linux Enterprise y debido también que la page cache se comparte entre contenedores y el host, la vulnerabilidad también permite impactos entre contenedores dockers y escenarios de escape de contenedores.

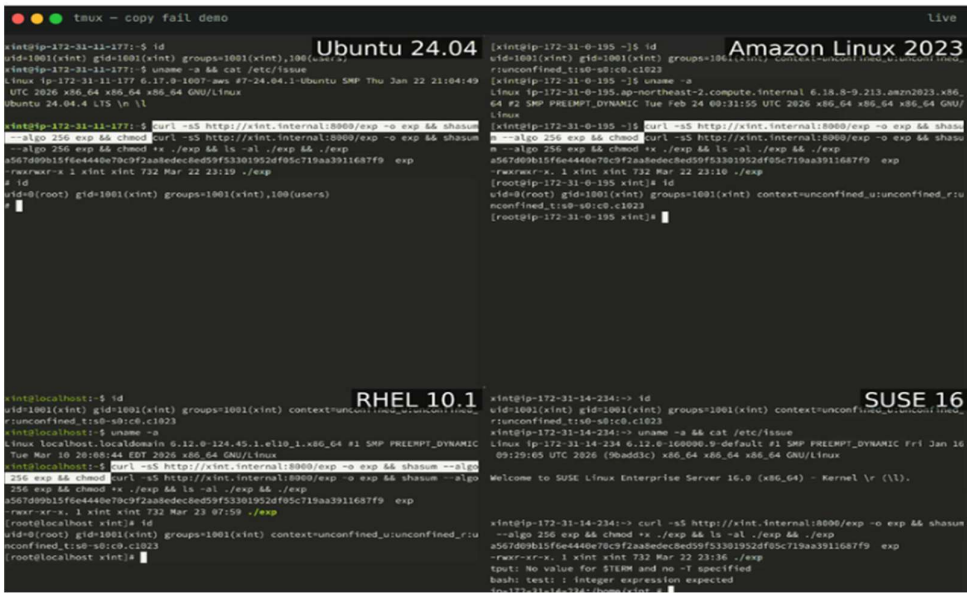

Figura 2.- Prueba del exploit en cuatro distribuciones de Linux devuelve una shell root - Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

IV. VECTOR DE ATAQUE

El vector es de tipo local CVSS: 3.1/AV: L/AC: H/PR: L/UI: N/S: C/C: H/I: H/A: H con una puntuación de 7.8.

Se detalla la cadena de explotación de Copy Fail:

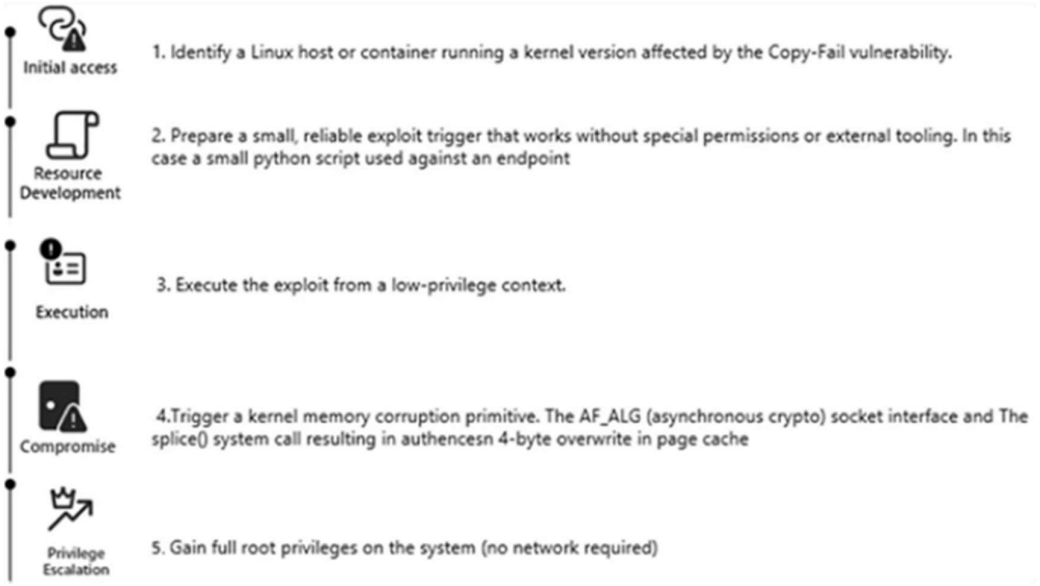

Figura 3.- Posible cadena de explotación de Copy Fail - Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

Fase Inicial: El atacante comienza con tareas de reconocimiento. Esto puede ocurrir tras obtener visibilidad limitada dentro de un entorno (por ejemplo, un *runner* de CI comprometido, un contenedor web o un host multi-tenant).

La información sobre la versión del kernel puede obtenerse fácilmente desde contenedores y espacios de nombres de usuario (*user namespaces*), sin necesidad de privilegios elevados. Dado que los contenedores comparten el kernel del host, una única versión vulnerable del kernel amplía inmediatamente el alcance del impacto desde un contenedor a todo el nodo.

Desarrollo de recurso: El atacante utiliza un script en Python que solo interactúa con funciones estándar del kernel accesibles para usuarios sin privilegios. No requiere co-

nexión a red, compilación, ni el uso de bibliotecas externas, por lo que puede ejecutarse fácilmente incluso en contenedores restringidos o entornos con fuertes medidas de seguridad.

Ejecución: El atacante ejecuta el script como un usuario sin privilegios en Linux, ya sea directamente en el host o desde un proceso comprometido dentro de un contenedor, sin necesidad de capacidades especiales. La vulnerabilidad no requiere privilegios de root dentro del contenedor, ni el uso de módulos del kernel o acceso a la red. Esto la convierte en una técnica especialmente efectiva en escenarios de post-explotación, donde el atacante ya cuenta con algún nivel inicial de acceso al sistema.

Compromiso: El exploit aprovecha la interacción entre la interfaz de sockets AF_ALG (criptografía asíncrona), la llamada al sistema `splice()` y un manejo incorrecto de errores durante una operación de copia fallida.

Como resultado, se produce una sobreescritura controlada de 4 bytes en la page cache del kernel. Esto permite al atacante, aun sin privilegios, corromper datos sensibles gestionados por el kernel. Dado que la manipulación ocurre completamente dentro del kernel, se eluden las protecciones tradicionales del espacio de usuario.

Escalada de privilegios: Al corromper estructuras del kernel asociadas a las credenciales o al contexto de ejecución, el atacante eleva su proceso a UID 0. Esto completa la transición de un usuario sin privilegios a root total sin necesidad de utilizar la red.

En este punto, los límites de confianza del kernel quedan comprometidos, las protecciones de SELinux/AppArmor se neutralizan de forma efectiva y los controles de seguridad locales son eludidos.

V. IMPACTO

Campo	Detalle
Ubuntu 24.04 LTS	Kernel 6.17.0-1007-aws
Amazon Linux 2023	Kernel 6.18.8-9.213.amzn2023
Red Hat Enterprise Linux (RHEL) 14.3	Kernel 6.12.2.0-124.45.1.el10_1
SUSE Linux Enterprise 16	Kernel 6.12.0-160000.9-default
WSL2 y contenedores Docker	Versiones no especificadas (potencialmente afectados)

Tabla 1.- Sistemas afectados - Vulnerabilidad crítica "Copy Fail" (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

VI. INDICADORES DE COMPROMISO

Exploit detectado MS Defender XDR
Linux/CopyFailExpDl.A
Python/CopyFail.A

Tabla 2.- Detecciones de Seguridad - Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

Campo	Detalle
URL	hxxps[:]//copy[.]fail/

Tabla 3.- URL asociada - Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

Tipo	Valor
MD5	75b009a56079eef56d8b845ffab385eb
SHA-1	83194d178f4b9c6fcdfaed0ea4ae3ec2ca3db6f4
SHA-256	a567d09b15f6e4440e70c9f2aa8edec8ed59f53301952df05c719aa3911687f9

Tabla 4.- Hashes - Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

Tipo	Nombre
Archivo	copy_fail_exp.py
Archivo	exploit.py
Archivo	copy_fail_exp.txt

Tabla 5.- Archivos Asociados - Vulnerabilidad crítica “Copy Fail” (CVE-2026-31431) permite escalada a privilegios root en kernel de Linux

VII. RECOMENDACIONES:

- Identifique todas las instancias de productos/versiones afectadas en su entorno.
- La solución principal es aplicar el parche del núcleo que revierte la optimización en el lugar de 2017 de algif_aead introducida por el commit a664bf3d603d de su sitio web https://git.kernel.org. Los proveedores de Linux ya están lanzando versiones parcheadas. Como medida de protección provisional, los administradores pueden:
    - Listar en la lista negra el moduo algif_aead a través de modprobe y eliminarlo el kernel en ejecución.

- Listar en la lista negra el modulo algif_aead y aplicar reglas de seccomp que bloqueen el uso de AF_ALG sockets.

- La monitorización también debe cubrir cambios sospechosos que involucren binarios setuid y patrones de ejecución que se asemejen a copy_fail_exp.py o comportamientos de explotación relacionados.
- Como una mitigación provisional para aquellos que aún no han recibido las actualizaciones, los investigadores recomiendan deshabilitar la interfaz criptográfica vulnerable, que bloquearía la creación de socket AF_ALG o deshabilitaría el módulo algif_aead mediante:

  - echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf
  - rmmod algif_aead

- Revise los registros para detectar signos de explotación con el UDO de EDR/XDR.
- Implementar el aislamiento de la red.
- Los investigadores de Theori sugieren tratar hosts Linux multi-tenant, clústeres de Kubernetes/container, corredores de CI/granjas de construcción y SaaS en la nube que ejecutan código de usuario como una prioridad en el esfuerzo de parcheo.
- Trate cualquier RCE de contenedor como posible compromiso de host y aplique el reciclaje rápido de nodos después de los indicadores de compromiso.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

MICROSOFT (2026). *CVE-2026-31431: Copy Fail vulnerability enables Linux root privilege escalation*. https://www.microsoft.com/en-us/security/blog/2026/05/01/cve-2026-31431-copy-fail-vulnerability-enables-linux-root-privilege-escalation/

SOC PRIME (2026). *CVE-2026-31431: Error de copia permite escalada de privilegios root en Linux*. https://socprime.com/es/active-threats/cve-2026-31431-error-de-copia-escalada-de-privilegios-root-linux/

XINT CODE RESEARCH TEAM (2026). *Copy Fail: 732 bytes to root on every major Linux distribution*. https://xint.io/blog/copy-fail-linux-distributions

CYBERSECURITY NEWS (2026). *Linux kernel 0-day Copy Fail vulnerability analysis*. https://cybersecuritynews.com/linux-kernel-0-day-copy-fail/

ADSLZONE (2026). *Vulnerabilidad Copy Fail en Linux permite acceso root*. https://www.adslzone.net/noticias/seguridad/vulnerabilidad-copy-fail-linux-cve-2026-31431/

LINUX ADICTOS (2026). *Copy Fail: la vulnerabilidad de Linux que abre la puerta al usuario root*. https://www.linuxadictos.com/copy-fail-la-vulnerabilidad-de-linux-que-abre-la-puerta-al-usuario-root.html