Boletín de alerta

Boletín Nro.:
Fecha de publicación: 30/04/2026
Tema: Alerta 2026-46 Vulnerabilidad Copy Fail en Linux
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Kernel de Linux, incluido en diversas distribuciones, tales como:
  - Ubuntu 24.04 LTS, kernel 6.17.0-1007-aws
  - Amazon Linux 2023, kernel 6.18.8-9.213.amzn2023
  - RHEL 10.1, kernel 6.12.0-124.45.1.el10_1
  - SUSE 16, kernel 6.12.0-160000.9-default

Descripción

Se ha identificado la vulnerabilidad CVE-2026-31431 en el Linux Kernel, relacionada con el manejo incorrecto de operaciones criptográficas dentro del componente algif_aead.

Diversos fabricantes y distribuidores Linux ya han comenzado a documentar el impacto. La vulnerabilidad tiene alta prioridad (CVSS 7.8) debido a que puede facilitar una escalación local de privilegios Lo relevante es que está presente en el propio kernel de Linux, lo que hace que afecte a prácticamente todas las distribuciones de Linux desde 2017 que se han desarrollado sobre dicho kernel.

De forma simplificada, la vulnerabilidad consiste en un error en cómo el kernel gestiona datos en memoria durante operaciones criptográficas, específicamente cuando se realizan procesos “in-place” (lectura y escritura en la misma ubicación de memoria). Este fallo puede provocar un comportamiento inesperado que puede ser aprovechado por un atacante.

Un usuario local sin privilegios podría explotar esta condición para manipular la memoria del kernel y elevar sus privilegios, obteniendo acceso a niveles más altos dentro del sistema, potencialmente hasta privilegios de administrador (root)

Reportes recientes también la identifican bajo el nombre “Copy Fail” y señalan la existencia de explotación pública.

Solución y mitigaciones:

Se recomiendan la siguientes acciones de forma inmediata:

- Aplicar las actualizaciones de kernel publicadas por la distribución correspondiente.
- Revisar advisories oficiales de Red Hat, Ubuntu, Debian, SUSE, Amazon Linux u otros proveedores afectados.
- Priorizar el parcheo en servidores críticos, sistemas multiusuario y plataformas de virtualización/contenedores.
- Como mitigación temporal, Ubuntu recomienda deshabilitar el módulo algif_aead cuando no sea requerido, hasta aplicar el parche correspondiente.

Información adicional:

- https://thehackernews.com/2026/04/new-linux-copy-fail-vulnerability.html
- https://xint.io/blog/copy-fail-linux-distributions
- https://copy.fail/
- https://github.com/tgies/copy-fail-c
- https://www.dynatrace.com/news/security-alert/local-privilege-escalation-vulnerability-copy-fail-cve-2026-31431/