# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 18/05/2026
**Tema:** Alerta 2026-52 Vulnerabilidad “DirtyDecrypt” en Kernel de Linux
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

Distribuciones Linux que utilicen kernels recientes con soporte habilitado para CONFIG_RXGK, incluyendo:

- Fedora Linux
- Arch Linux
- openSUSE Tumbleweed

## Descripción

Se ha identificado una vulnerabilidad de escalación de privilegios conocida como **DirtyDecrypt** o **DirtyCBC** , relacionada con el módulo **rxgk** del kernel de Linux.

La vulnerabilidad permite que un usuario local obtenga privilegios elevados, potencialmente acceso **root**, comprometiendo la seguridad del sistema afectado.

Aunque actualmente no cuenta con un identificador CVE oficial confirmado, diversos investigadores la relacionan con la vulnerabilidad CVE-2026-31635.

El fallo afecta principalmente sistemas Linux que tengan habilitada la opción de configuración:

- CONFIG_RXGK

La vulnerabilidad ya cuenta con una **prueba de concepto pública (PoC)**, lo que incrementa el riesgo de explotación en entornos vulnerables.

## Solución:

- Actualizar inmediatamente el kernel de Linux a la versión más reciente proporcionada por el fabricante o distribución utilizada.
- En caso de no poder actualizar de inmediato, se recomienda deshabilitar temporalmente los módulos vulnerables mediante el siguiente comando:

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»

## Información adicional:

- https://www.bleepingcomputer.com/news/security/exploit-available-for-new-dirtydecrypt-linux-root-escalation-flaw/
- https://github.com/v12-security/pocs/tree/main/dirtydecrypt