La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) incorporó el viernes una vulnerabilidad de seguridad recientemente revelada, que afecta a múltiples distribuciones de Linux, a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), señalando que ya existen evidencias de explotación activa en entornos reales.

La falla, identificada como CVE-2026-31431 (con una puntuación CVSS de 7.8), corresponde a una vulnerabilidad de escalamiento local de privilegios (LPE) que podría permitir a un usuario local sin privilegios obtener acceso root. Este fallo, que ha estado presente durante nueve años, también es conocido como Copy Fail por los investigadores de Theori y Xint. Ya se han publicado correcciones en las versiones del kernel de Linux 6.18.22, 6.19.12 y 7.0.

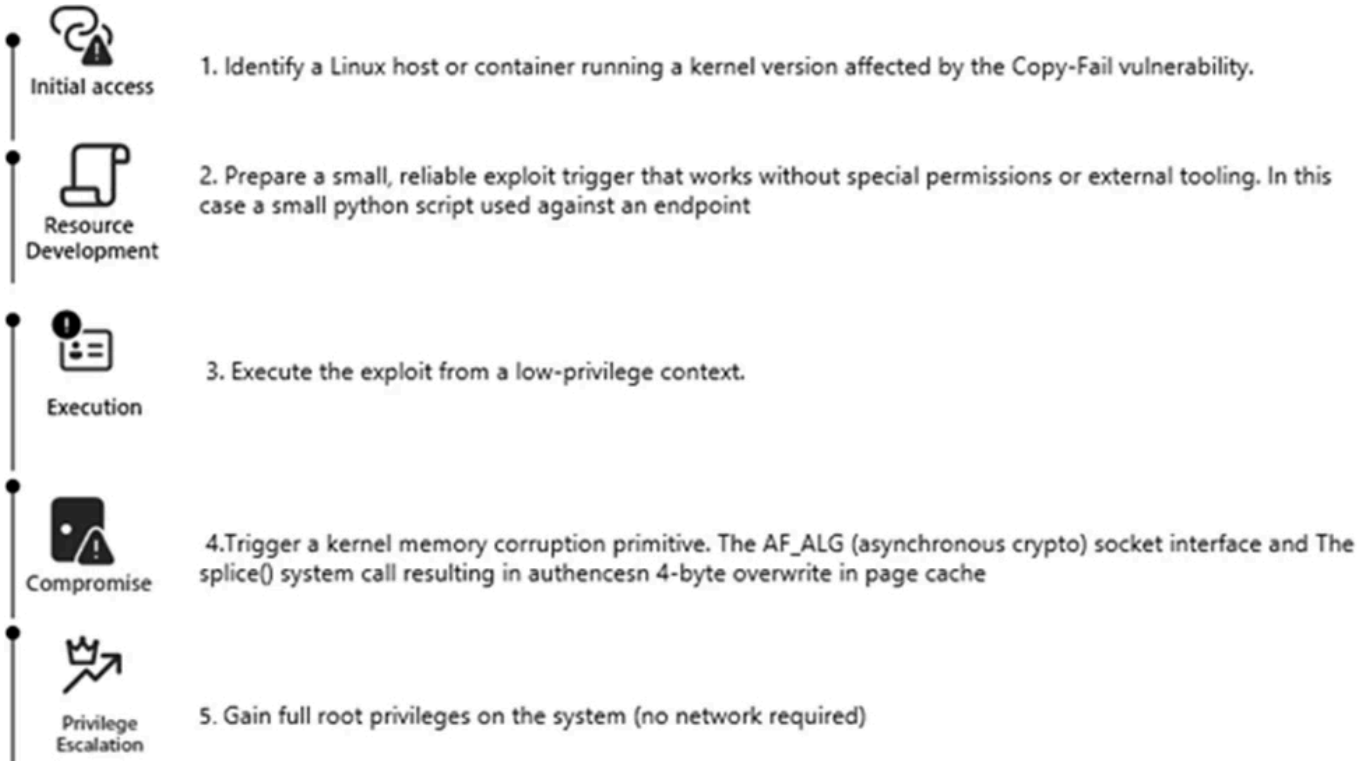
«El kernel de Linux contiene una vulnerabilidad relacionada con una transferencia incorrecta de recursos entre dominios, lo que podría facilitar la escalada de privilegios,» indicó CISA en un comunicado.

En un informe publicado a principios de esta semana, los investigadores explicaron que Copy Fail surge de un error lógico en la plantilla criptográfica de autenticación del kernel de Linux, lo que permite a un atacante provocar de manera confiable una escalada de privilegios mediante un exploit sencillo de 732 bytes escrito en Python. Este problema se originó a partir de tres cambios independientes en el kernel realizados en 2011, 2015 y 2017, los cuales, de forma individual, no representaban un riesgo.

Esta vulnerabilidad de alta gravedad afecta a distribuciones de Linux publicadas desde 2017 y permite que un usuario local sin privilegios obtenga acceso a nivel root al corromper la caché de páginas en memoria del kernel correspondiente a cualquier archivo legible, incluyendo binarios con el bit setuid. Dicha manipulación puede ser realizada por usuarios sin privilegios y puede derivar en la ejecución de código con permisos de root.

«Debido a que la caché de páginas representa la versión en memoria de los ejecutables, modificarla equivale a alterar los binarios en el momento de su ejecución sin modificar el disco,» explicó Wiz, empresa propiedad de Google. *«Esto permite a los atacantes inyectar código en binarios privilegiados (por ejemplo, /usr/bin/su) y así obtener privilegios de root.»*

La amplia adopción de Linux en entornos de nube amplifica el impacto de esta vulnerabilidad. En su análisis, Kaspersky indicó que Copy Fail representa un riesgo significativo para entornos basados en contenedores, ya que Docker, LXC y Kubernetes *«permiten que los procesos dentro de un contenedor accedan al subsistema AF_ALG si el módulo algif_aead está cargado en el kernel del host»* de forma predeterminada.



«Copy Fail implica un riesgo de romper el aislamiento de contenedores y tomar control de la máquina física,» señaló la compañía rusa. *«Además, su explotación no requiere técnicas complejas como condiciones de carrera o la adivinación de direcciones de memoria, lo que reduce considerablemente la barrera de entrada para un atacante.»*

«Detectar este ataque resulta complicado porque el exploit utiliza únicamente llamadas al sistema legítimas, difíciles de distinguir del comportamiento normal de las aplicaciones.»

La urgencia aumenta debido a la disponibilidad de una prueba de concepto (PoC) completamente funcional. Kaspersky indicó que ya se han encontrado versiones en Go y Rust basadas en la implementación original en Python dentro de repositorios de código abierto.

CISA no proporcionó detalles sobre cómo se está explotando la vulnerabilidad en escenarios reales. No obstante, el equipo de investigación de seguridad de Microsoft Defender afirmó que *«se están observando actividades preliminares de prueba que probablemente deriven en un incremento de explotación por parte de actores maliciosos en los próximos días.»*

«El vector de ataque es local (AV:L) y requiere bajos privilegios sin interacción del usuario, lo que significa que cualquier usuario sin privilegios en un sistema vulnerable puede intentar explotarlo,» añadieron. *«Es importante destacar que esta vulnerabilidad no puede ser explotada de forma remota por sí sola, pero adquiere un alto impacto cuando se combina con un acceso inicial, como acceso por SSH, ejecución de trabajos CI maliciosos o compromisos en contenedores.»*

El gigante tecnológico también describió una posible cadena de ataque que los actores maliciosos podrían seguir para explotar la vulnerabilidad:

- Realizar reconocimiento para identificar un sistema Linux o contenedor que ejecute una versión del kernel vulnerable a Copy Fail.
- Preparar un pequeño script en Python para atacar el objetivo.
- Ejecutar el exploit desde un contexto de bajos privilegios, ya sea como un usuario estándar en el host o desde un contenedor comprometido sin capacidades especiales.
- El exploit realiza una sobrescritura controlada de 4 bytes en la caché de páginas del kernel, provocando la corrupción de datos sensibles gestionados por este.
- El atacante eleva su proceso a UID 0 y obtiene privilegios completos de root.

Las agencias del Federal Civilian Executive Branch (FCEB) han sido instadas a aplicar las actualizaciones antes del 15 de mayo de 2026, ya que las distribuciones afectadas han comenzado a liberar parches. En caso de no poder aplicar las correcciones de inmediato, se recomienda desactivar la funcionalidad afectada, implementar aislamiento de red y reforzar

los controles de acceso.