

Boletín de alerta

Boletín Nro.: 112

Fecha de publicación: 30/09/2026

Tema: Alerta 2026-112 Vulnerabilidad sin parche de Ubuntu permite escape de contenedores y root en el host

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto / plataforma	Estado
Ubuntu 22.04 LTS	Potencialmente afectado; sin actualización de kernel de Ubuntu publicada al momento del reporte
Ubuntu 24.04 LTS	Potencialmente afectado; sin actualización de kernel de Ubuntu publicada al momento del reporte
Ubuntu 26.04	Afectado; exploit público demostrado para esta versión
Hosts Linux con kernel vulnerable y uso de contenedores	Potencialmente afectados; validar versión de kernel y backports del fabricante
Linux upstream	Corregido en Linux 7.2 y Linux 7.1.10

La condición de exposición depende del kernel realmente ejecutado y de los *backports* aplicados por cada distribución. Un número de versión inferior a Linux 7.1.10 o 7.2 no confirma por sí solo que el host sea vulnerable si el proveedor ya incorporó el parche en un kernel mantenido; se debe validar contra los avisos de seguridad del fabricante.

Descripción

Se identificó **CVE 2026 80521**, una vulnerabilidad de alta severidad en el kernel de Linux que afecta el subsistema de sockets **AF_UNIX** y puede permitir que un atacante con ejecución local dentro de un contenedor escape hacia el sistema anfitrión y obtenga privilegios **root**. La falla tiene una puntuación **CVSS 7.8** y existe código de explotación público dirigido a **Ubuntu 26.04**.

Aunque el defecto fue corregido en el kernel Linux *upstream* el 6 de agosto de 2026 e incluido en Linux 7.2 y Linux 7.1.10, al momento de los reportes Ubuntu todavía no había distribuido una actualización de kernel que corrigiera el problema para **Ubuntu 22.04 LTS, 24.04 LTS y 26.04**. No existe un *workaround* oficial completo, por lo que deben aplicarse controles compensatorios hasta que Canonical publique el paquete corregido.

La vulnerabilidad no permite comprometer un host remoto directamente desde Internet. El atacante necesita ejecutar código previamente dentro de un contenedor. Sin embargo, una vez que obtiene ese acceso inicial —por ejemplo, mediante una aplicación web vulnerable, imagen maliciosa, credenciales expuestas, canal CI/CD comprometido o ejecución de comandos en un *pod*— puede utilizar el fallo para cruzar la frontera de aislamiento y obtener control administrativo sobre el nodo anfitrión.

Acciones inmediatas

Mientras se espera la publicación de la actualización de parte del equipo de Ubuntu, puede seguir las siguientes recomendaciones:

1. **Identificar todos los hosts Ubuntu que ejecuten cargas de contenedores.** Incluir nodos Kubernetes, servidores Docker/containerd, LXD/LXC, *runners* CI/CD, plataformas PaaS, ambientes de desarrollo, staging, producción y recuperación ante desastres.
2. **Monitorear los avisos de Canonical/Ubuntu y aplicar inmediatamente el primer kernel corregido disponible** para Ubuntu 22.04 LTS, 24.04 LTS y 26.04. La corrección upstream está presente en Linux 7.2 y 7.1.10, pero el paquete corregido dependerá de cada rama y canal de kernel
Ubuntu.computerhoy.20minutos+1
3. **No ejecutar cargas de trabajo no confiables en hosts afectados.** Suspender temporalmente la ejecución de imágenes de terceros no validadas, contenedores proporcionados por clientes, *runners* compartidos y pruebas de código no confiable en nodos que también alojan servicios críticos.
4. **Eliminar contenedores privilegiados y privilegios innecesarios.** Prohibir privileged: true, evitar hostPID, hostNetwork, hostIPC, montajes hostPath, acceso a /var/run/docker.sock y capacidades Linux no requeridas.
5. **Aplicar políticas restrictivas en Kubernetes.** Usar Pod Security Admission en modo restricted, Kyverno, OPA Gatekeeper u otros mecanismos para bloquear contenedores privilegiados, montajes de host y *capabilities* peligrosas.
6. **Separar cargas críticas de cargas no confiables.** Evitar que control plane, aplicaciones de identidad, bases de datos, sistemas de seguridad, herramientas de monitoreo o datos sensibles compartan nodo con contenedores de menor confianza.
7. **Usar aislamiento reforzado cuando sea posible.** Priorizar gVisor, Kata Containers, Firecracker/microVMs, nodos dedicados o máquinas virtuales separadas para cargas multi-tenant, expuestas a Internet o procedentes de terceros.
8. **Restringir acceso a los nodos.** Limitar SSH, cuentas administrativas, acceso desde CI/CD y ejecución remota a identidades aprobadas, MFA, *jump hosts* y redes de administración segmentadas.
9. **Fortalecer la detección.** Monitorizar escaladas de privilegios, procesos ejecutados como root, uso anómalo de sockets AF_UNIX, acceso a /proc, montajes inesperados, modificaciones de *capabilities*, accesos a sockets Docker/containerd y conexiones salientes no autorizadas desde nodos.
10. **Realizar revisión de compromiso** en nodos con cargas vulnerables o no confiables. Buscar creación de usuarios, cambios de *cron*, servicios o módulos de kernel, procesos root desconocidos, modificaciones de configuraciones, accesos anómalos a secretos y actividad lateral desde el host.

Información adicional:

- <https://thehackernews.com/2026/09/exploit-released-for-unpatched-ubuntu.html>
- https://computerhoy.20minutos.es/software/detectan-un-grave-error-kernel-ubuntu-con-puntuacion-cvss-7-8-que-canonical-todavia-no-ha-sido-capaz-solucionar_7042115_0.html
- <https://blog.elhacker.net/2026/09/grave-error-sin-solucion-en-kernel-de.html>