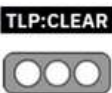


Nro. Alerta:	AL-2026-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
		ALERTAS DE SEGURIDAD	V 1.1
Fecha:	2-oct-2026	Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521	Pág.: 1 of 6

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Explotación de vulnerabilidad
Nivel de riesgo: Alta

II. ALERTA



Figura 1.- Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521 - figura referencial

La empresa de ciberseguridad DepthFirst informó sobre la vulnerabilidad CVE-2026-80521 junto con un exploit que afecta a Ubuntu 26.04. El fallo es del tipo uso después de la liberación (use-after-free) y se encuentra en el mecanismo de recolección de basura de los sockets AF_UNIX del kernel de Linux. La vulnerabilidad puede ser explotada por un proceso sin privilegios que se ejecute dentro de un contenedor Docker o Kubernetes, permitiendo escapar del contenedor y obtener privilegios de root (administrador) en el sistema anfitrión (host).

III. INTRODUCCIÓN

DepthFirst afirma haber identificado la vulnerabilidad CVE-2026-80521 mediante un modelo de IA propio denominado "dfs-large1", junto con un sistema personalizado de fuzzing y explotación. El 22 de septiembre de 2026 publicó su informe de investigación titulado "Containers Are No Longer a Security Boundary" ("Los contenedores ya no son una barrera de seguridad"), basado sobre CVE-2026-80521 junto con la liberación en GitHub de un exploit 0-day dirigido a Ubuntu 26.04.



Nro. Alerta:	AL-2026-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 V 1.1
TLP:			
Fecha:	2-oct-2026	Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521	Pág.: 2 of 6

```

// Conceptual illustration only -- not functional exploit code
Thread A: socket.send(fd_via_SCM_RIGHTS) // builds SCC edge in GC graph
Thread B: socket.close()                // triggers unix_del_edge()
                                           // scc_entry NOT unlinked (the bug)
GC pass: walks graph, frees unix_vertex // struct freed while still referenced
Thread A: kernel dereferences stale vertex // use-after-free triggered

```

Figura 2. - Pseudocódigo de ilustración simplificada y no funcional del intervalo de tiempo de CVE-2026-80521

La relevancia de CVE-2026-80521 radica en que rompe una de las premisas fundamentales del modelo de seguridad de los entornos de contenedores multiinquilino (*multi-tenant*): que un proceso ejecutado dentro de un contenedor no puede obtener privilegios de *root* sobre el kernel del sistema anfitrión. La vulnerabilidad afecta a instalaciones Ubuntu con configuraciones estándar y sin modificaciones, y se basa en una falla de tipo *heap use-after-free*, una categoría de vulnerabilidades que los equipos de seguridad del kernel han intentado mitigar y erradicar durante más de una década.

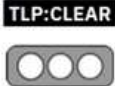
La vulnerabilidad subyacente del kernel de Linux había sido corregida en la rama principal (*upstream*) el 6 de agosto de 2026; sin embargo, Ubuntu aún no había distribuido el parche para algunas de sus versiones LTS afectadas. Al 24 de septiembre de 2026, el sistema de seguimiento de seguridad de Ubuntu continuaba clasificando el paquete principal del kernel de Ubuntu 26.04 LTS con el estado "Vulnerable, work in progress" (vulnerable, corrección en desarrollo).

IV. VECTOR DE ATAQUE

CVE-2026-80521 posee una nivel de severidad ALTA con puntuación 7.8 de tipo LOCAL, CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

La vulnerabilidad de tipo uso después de liberación (*use-after-free*) en el heap del subsistema AF_UNIX del kernel de Linux. La vulnerabilidad se origina por una condición de carrera (*race condition*), en la que dos operaciones del kernel se superponen o se ejecutan de forma concurrente cuando no deberían, durante la gestión y limpieza de determinados objetos relacionados con los sockets UNIX.



Nro. Alerta:	AL-2026-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
		ALERTAS DE SEGURIDAD	V 1.1
Fecha:	2-oct-2026	Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521	Pág.: 3 of 6

Estos sockets son un mecanismo utilizado desde hace décadas que permite a los procesos que se encuentran en la misma máquina intercambiar datos. Además, admiten una función denominada SCM_RIGHTS, que permite que un proceso transfiera un descriptor de archivo abierto a otro proceso a través del socket.

Durante esta transferencia de descriptores de archivos, el kernel publica nuevas referencias para que sean procesadas por el recolector de basura justo antes de poner el mensaje en cola. Estas referencias entre sockets son representadas internamente mediante objetos unix_vertex, que permiten al recolector de basura del kernel realizar el seguimiento de las relaciones entre los sockets.

Cuando varios de estos objetos están conectados mediante referencias que forman un ciclo, constituyen un Strongly Connected Component (SCC). Si el recolector se ejecuta durante el intervalo en el que las nuevas referencias todavía están siendo procesadas y el mensaje aún no ha sido puesto en cola, pueden analizar las referencias en un estado inconsistente y considerar que determinados objetos del SCC ya no son alcanzables, provocando la liberación de parte de ellos.

Como consecuencia de la condición de carrera, un objeto unix_vertex puede ser liberado mientras todavía existe una referencia hacia él. El objeto liberado puede permanecer vinculado en el anillo de caché asociado al scc_entry de un objeto superviviente. En una ejecución posterior del recolector, este puede acceder al unix_vertex mediante esa referencia que todavía existe, aunque la memoria ya haya sido liberada.

Ese acceso a un objeto después de que su memoria haya sido liberada es precisamente lo que constituye la vulnerabilidad use-after-free (UAF), la cual puede provocar corrupción de memoria y denegación de servicio y bajo determinadas condiciones de explotación, permitir escalamiento de privilegios.

V. IMPACTO

El rastreador de seguridad de Canonical, que es utilizado para registrar y dar seguimiento a las vulnerabilidades de seguridad que afectan a Ubuntu, confirma afectación en el paquete principal del kernel de:

Nro. Alerta:	AL-2026-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 V 1.1
TLP:			
Fecha:	2-oct-2026	Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521	Pág.: 4 of 6

Distribución	Estado
Ubuntu 26.04 LTS	Afectado
Ubuntu 24.04 LTS	Afectado
Ubuntu 22.04 LTS	No afectado en el paquete estándar linux-generic*

Tabla 1.- Estado de afectación de Ubuntu frente a CVE-2026-80521

Canonical también indica que el paquete estándar linux de Ubuntu 22.04 LTS no se encuentra afectado. Sin embargo, Ubuntu ofrece diferentes variantes del kernel, además del kernel genérico (generic), por lo que la afectación debe determinarse según la variante y versión específica del kernel instalado Ubuntu 22.04.

En el kernel de Linux, el upstream que es el proyecto principal del kernel Linux, donde se desarrollan e incorporan originalmente nuevas funcionalidades, correcciones de errores y parches de seguridad informa que el código vulnerable se introdujo en:

Rama / versión	Descripción
Kernel 6.10	Introducción del código vulnerable
Kernel 6.1	Código vulnerable adaptado (<i>backported</i>)
Kernel 6.6	Código vulnerable adaptado (<i>backported</i>)

Tabla 2.- Ramas del kernel Linux asociadas a CVE-2026-80521

La falla no se limita a las instalaciones ordinarias de Ubuntu, Canonical mantiene paquetes de kernel de Linux separados para entornos de infraestructura, por lo que también requieren atención, estos incluyen:

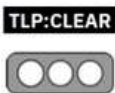
Entorno / plataforma
AWS
Microsoft Azure
Google Cloud
Oracle
KVM
Plataformas de hardware especializadas

Tabla 3.- Entornos de infraestructura con paquetes de kernel que requieren revisión

VI. INDICADORES DE COMPROMISO

- Actividad anómala originada desde contenedores hacia interfaces o funcionalidades del kernel que utilicen AF_UNIX.



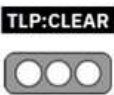
Nro. Alerta:	AL-2026-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
		ALERTAS DE SEGURIDAD	V 1.1
Fecha:	2-oct-2026	Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521	Pág.: 5 of 6

- Procesos ejecutados desde contenedores que obtengan inesperadamente privilegios elevados en el sistema host.
- Creación o ejecución inesperada de procesos con privilegios root.
- Cambios no autorizados en archivos, configuraciones o mecanismos de persistencia del sistema host.
- Reinicios, kernel panics, errores o comportamientos anómalos relacionados con el kernel.
- Actividad inusual relacionada con operaciones de sockets UNIX y transferencia de descriptores mediante SCM_RIGHTS

VII. RECOMENDACIONES:

- Aplicar las actualizaciones del Linux Kernel a la 7.2 y 7.1.10 proporcionadas por Ubuntu/Canonical o por la distribución utilizada.
- Identificar los sistemas que ejecuten versiones vulnerables del kernel.
- Priorizar servidores que ejecuten Docker, Kubernetes u otras plataformas de contenedores, especialmente cuando procesen cargas de trabajo no confiables.
- Mantener los sistemas de contenedores y sus componentes de aislamiento actualizados.
- Aplicar el principio de mínimo privilegio en contenedores y evitar capacidades privilegiadas innecesarias.
- Revisar y reforzar los perfiles seccomp, AppArmor y otros mecanismos de aislamiento disponibles.
- Evitar el uso de contenedores privilegiados cuando no sea estrictamente necesario.
- Revisar los sistemas host en busca de procesos, archivos o modificaciones realizadas con privilegios root que no correspondan a la actividad esperada.
- En caso de identificar evidencias compatibles con explotación, realizar análisis forense del host y de los contenedores afectados antes de considerarlos confiables.
- Mantener seguimiento de los avisos de seguridad publicados por Ubuntu/Canonical y del estado de los paquetes corregidos.



Nro. Alerta:	AL-2026-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	2-oct-2026	Vulnerabilidad de alta severidad en Ubuntu 26.04 permite escape de contenedores – CVE-2026-80521	Pág.: 6 of 6

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:

TECH-INSIDER. (2026). *CVE-2026-80521: Linux Container Escape to Root.* <https://tech-insider.org/cve-2026-80521-linux-container-escape-root-2026/>

THE HACKER NEWS. (2026). *Exploit Released for Unpatched Ubuntu 26.04 Container Escape Vulnerability.* <https://thehackernews.com/2026/09/exploit-released-for-unpatched-ubuntu.html>

LINUX JOURNAL. (2026). *Ubuntu Container Escape Vulnerability Gets Public Exploit, Kernel Patch Arrives.* <https://www.linuxjournal.com/content/ubuntu-container-escape-vulnerability-gets-public-exploit-kernel-patch-arrives>

CYBER KENDRA. (2026). *CVE-2026-80521: Ubuntu Container Escape Exploit.* <https://www.cyberkendra.com/2026/09/cve-2026-80521-ubuntu-container-escape-exploit.html>

