Nro. Alerta:	AL-2026-016	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	27-mar-2026	Vulnerabilidad CVE-2026-3888 en sistemas Ubuntu	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Escalada de privilegios en sistemas Linux
Nivel de riesgo: Alta

II. ALERTA

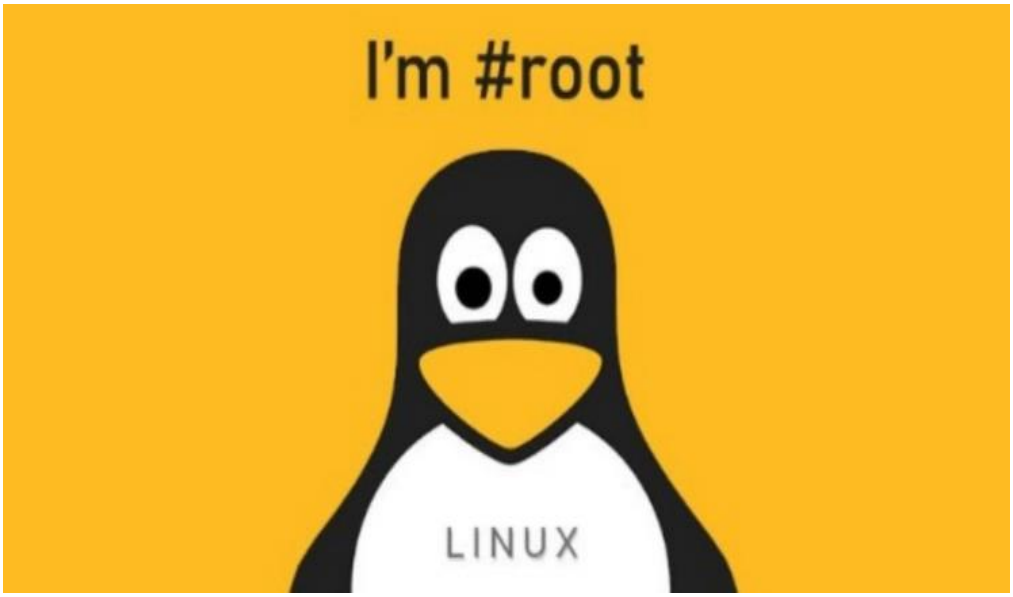

Figura 1.- Vulnerabilidad CVE-2026-3888 en sistemas Ubuntu - figura referencial

Se ha identificado una vulnerabilidad crítica en instalaciones por defecto de Ubuntu Desktop versión 24.04 y posteriores, denominada CVE-2026-3888, la cual permite a un usuario local sin privilegios escalarlo a usuario con privilegios root por medio de la interacción de 2 componentes estándar snap-confine y systemd-tmpfiles.

III. INTRODUCCIÓN

Snapd es el servicio (daemon) que gestiona todo el sistema de paquetes Snap en Ubuntu, desde descubrimiento, instalación, actualizaciones, la eliminación de paquetes snap, aplicaciones autocontenidas que incluyen sus propias dependencias en lugar de depender de bibliotecas compartidas del sistema. Canonical diseñó este formato para resolver conflictos de dependencias y ofrecer a los desarrolladores un único objetivo de empaquetado para distintas versiones de Ubuntu. Además, snapd aplica el modelo de permisos que controla a qué puede acceder

cada snap en el sistema anfitrión, por lo que actúa tanto como gestor de paquetes como motor de políticas de seguridad.

La Unidad de Investigación de Amenazas de Qualys identifico la falla CVE-2026-3888 que es una vulnerabilidad de Escalada de Privilegios Locales (LPE) en Ubuntu Desktop 24.04 permitiendo a un usuario local alcanzar y poder ejecutar acciones de un usuario root, dicha falla depende de 2 componentes:

- Snap-confine es un componente de seguridad de encargado de crear y aislar el entorno de ejecución de las aplicaciones (sandbox) en la ruta /tmp/.snap de Snap.
- Systemd-tmpfiles es una herramienta del sistema (systemd) que se encarga de crear archivos y directorios temporales como /tmp, /run o /var/tmp, establecer permisos, limpiar archivos antiguos e inicializar rutas necesarias al arrancar el sistema.

Además, durante la investigación se encontró en Ubuntu Desktop 25.10 en el paquete uutils coreutis una condición de ejecución en la utilidad rm, que permitía a un atacante local sin privilegios sustituir entradas de directorio por enlaces simbólicos durante la ejecución de tareas cron propiedad de root (específicamente, /etc/cron.daily/apport). La explotación exitosa podría dar lugar a la eliminación arbitraria de archivos como root o a una mayor escalada de privilegios al atacar los directorios de la zona de pruebas de snap.

IV. VECTOR DE ATAQUE

La vulnerabilidad yace cuando la política de limpieza de systemd realiza la limpieza automática y programada de los directorios temporales /tmp incluido la /tmp/.snap, en la cual un atacante puede aprovechar esta ventana para crear una estructura o payloads maliciosos en /tmp/.snap con permisos manipulados, propietarios incorrectos.

Luego cuando snap-confine vuelve a interactuar con esa ruta durante la inicialización del entorno y si se cumplen las condiciones de inicio y permisos implicados, la cadena puede terminar derivando en ejecución con privilegios elevados.

Este exploit no es instantáneo, puesto que la programación de limpieza de systemd-tmpfiles en Ubuntu 24.04 tiene un margen de 30 días, mientras que en versiones posteriores es de 10 días.

El vector es de tipo local CVSS: 3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H con una puntuación de 7.8.

V. IMPACTO

Las versiones del paquete snapd detalladas a continuación presentan vulnerabilidades, por lo que se recomienda su actualización inmediata a las versiones corregidas indicadas.

Sistema / Versión	Condición de vulnerabilidad
Ubuntu 24.04 LTS	Versiones de snapd anteriores a 2.73+ubuntu24.04.2
Ubuntu 25.10 LTS	Versiones de snapd anteriores a 2.73+ubuntu25.10.1
Ubuntu 26.04 LTS (Desarrollo)	Versiones de snapd anteriores a 2.74.1+ubuntu26.04.1
Snapd (rama principal)	Versiones anteriores a 2.75

Tabla 1.- Versiones Afectadas - Vulnerabilidad CVE-2026-3888 en sistemas Ubuntu

En sistemas heredados (Ubuntu 16.04 a 22.04 LTS), aunque no son vulnerables por defecto, se recomienda aplicar los parches como medida preventiva ante configuraciones no estándar.

Para sistemas con Ubuntu Desktop 24.04 o superior, se requiere la actualización inmediata.

VI. INDICADORES DE COMPROMISO

- Ubuntu 24.04 o posterior
- Servicio Snapd
- Ruta comprometida /tmp/.snap

VII. RECOMENDACIONES:

- Aplicar los parches de seguridad oficiales del sistema operativo de manera oportuna.
- Mantener actualizado el paquete snapd a versiones corregidas y seguras.
- Limitar el acceso local únicamente a usuarios autorizados y confiables.
- Implementar el principio de mínimo privilegio en todas las cuentas de usuario.
- Supervisar actividades sospechosas en directorios como /tmp, /run y /var/tmp.
- Auditar eventos relacionados con la ejecución de procesos con privilegios elevados.

- Configurar y revisar los mecanismos de limpieza automática mediante systemd-tmpfiles.
- Implementar controles de integridad de archivos (FIM) para detectar modificaciones no autorizadas.
- Segmentar los entornos críticos y restringir el acceso a sistemas sensibles.

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:

UBUNTU (2026). Vulnerabilidad de seguridad CVE-2026-3888. https://ubuntu.com/security/CVE-2026-3888

INCIBE-CERT (2026). Vulnerabilidad CVE-2026-3888 en sistemas Ubuntu. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2026-3888

HISPASEC (2026). CVE-2026-3888 en Ubuntu: escalada a root aprovechando snap-confine y systemd-tmpfiles. https://unaaldia.hispasec.com/2026/03/cve-2026-3888-en-ubuntu-escalada-a-root-aprovechando-snap-confine-y-la-limpieza-de-systemd-tmpfiles.html

QUALYS (2026). Important Snap flaw enables local privilege escalation to root (CVE-2026-3888). https://blog.qualys.com/vulnerabilities-threat-research/2026/03/17/cve-2026-3888-important-snap-flaw-enables-local-privilege-escalation-to-root

FEVAR54 (2026). Proof of Concept CVE-2026-3888 desde la plataforma Qualys. https://github.com/fevar54/CVE-2026-3888-POC-all-from-the-Qualys-platform