GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición °1126

## BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

## VISTA RÁPIDA

| | CRÍTICO | URGENTE | IMPORTANTE |
|---|---|---|---|
| **VULNERABILIDADES** | 2 | 1 | 0 |
| **MALWARE** | 0 | 1 | 0 |
| **NOTICIAS DE CIBERSEGURIDAD** | 0 | 0 | 1 |

## VULNERABILIDADES

### CANONICAL UBUNTU — ESCALADA DE PRIVILEGIOS LOCAL EN SNAPD (CVE-2026-3888)

Canonical ha alertado sobre una vulnerabilidad crítica de escalada de privilegios local (LPE) que afecta a las instalaciones por defecto de Ubuntu Desktop y Server. El fallo permite a un atacante con acceso limitado al sistema obtener privilegios de root mediante la explotación de una condición de carrera en la gestión de directorios temporales, lo que deriva en el compromiso total del host afectado.

**Resumen técnico:**

- Identificador principal: CVE-2026-3888.
- Severidad: 7.8 (Alta) según la escala CVSSv3.1.
- Causa raíz: Interacción insegura entre los componentes snap-confine (binario setuid root) y systemd-tmpfiles durante la limpieza de directorios en /tmp.
- Mecanismo de falla: El exploit aprovecha la ventana temporal en la que systemd-tmpfiles elimina el directorio privado /tmp/.snap. Un atacante puede recrear esta estructura con punteros maliciosos antes de que snap-confine realice el montaje (bind-mount), logrando que el sistema ejecute código arbitrario con privilegios elevados.
- Estado de explotación: Vulnerabilidad pública confirmada; existe código de prueba de concepto (PoC) detallado por investigadores de Qualys, aunque no se reporta explotación masiva activa al día de hoy.
- Versiones afectadas: Ubuntu Desktop/Server (16.04, 18.04, 20.04, 22.04, 24.04 LTS y 25.10) con snapd en versiones anteriores a la 2.75.

**Impacto potencial:**

- Control total del sistema: Un usuario local sin privilegios puede elevarse a superusuario (root), permitiendo el acceso irrestricto a todo el sistema operativo.
- Evasión de sandboxing: Compromiso de las políticas de aislamiento de AppArmor y seccomp que normalmente confinan a las aplicaciones Snap.
- Persistencia avanzada: Capacidad del atacante para instalar backdoors, exfiltrar credenciales del sistema o modificar registros críticos sin dejar rastro evidente.
- Compromiso de integridad: Alteración de binarios del sistema y archivos de configuración que dependen de la estructura de snapd.

**Recomendaciones de mitigación:**

1. Actualización inmediata de snapd: Aplicar los parches de seguridad de Canonical actualizando el paquete a la versión corregida (ej. 2.73+ubuntu24.04.2 para Noble o 2.75 para versiones upstream).
2. Verificación de versiones: Ejecutar el comando dpkg -l snapd en las terminales para confirmar que la versión instalada es igual o superior a las versiones parchadas reportadas por el equipo de seguridad de Ubuntu.
3. Endurecimiento de configuración (Workaround): En sistemas donde no sea posible actualizar, modificar manualmente /usr/lib/tmpfiles.d/snapd.conf para restringir la limpieza automática de los directorios privados de snap.
4. Auditoría de logs y archivos temporales: Implementar reglas de monitoreo para detectar cambios de propietario o recreaciones sospechosas de directorios en la ruta /tmp/snap-private-tmp.

**Prioridad: Urgente.**

**Ampliar información:**

- https://discourse.ubuntu.com/t/snapd-local-privilege-escalation-cve-2026-3888/78627
- https://thehackernews.com/2026/03/ubuntu-cve-2026-3888-bug-lets-attackers.html
- https://blog.qualys.com/vulnerabilities-threat-research/2026/03/17/cve-2026-3888-important-snap-flaw-enables-local-privilege-escalation-to-root
- https://unaaldia.hispasec.com/2026/03/cve-2026-3888-en-ubuntu-escalada-a-root-aprovechando-snap-confine-y-la-limpieza-de-systemd-tmpfiles.html/amp
- https://ubuntu.com/security/CVE-2026-3888

## CVE-2026-3888 Ubuntu - Local Privilege Escalation in snapd

Se ha publicado que la vulnerabilidad que permite la escalada de privilegios locales en snapd en Ubuntu en Linux, permitiendo a atacantes locales obtener privilegios de root al recrear el directorio privado /tmp de snap cuando systemd-tmpfiles está habilitado para limpiar automáticamente este directorio.

**Resumen técnico:**

- Identificadores principales: CVE-2026-3888
- Severidad: High (Puntajes CVSS de 7.8).
- Causa raíz: La raíz del problema está en una interacción inesperada entre dos componentes muy comunes en estas instalaciones. Por un lado, **snap-confine**, pieza clave de **snapd** que se encarga de preparar el sandbox y aislar las aplicaciones **Snap**; por otro, **systemd-tmpfiles**, el mecanismo de **systemd** que aplica políticas de limpieza automática en directorios temporales como **/tmp**, **/run** o **/var/tmp**. El escenario descrito se apoya en el manejo del directorio **/tmp/.snap**: cuando la política de limpieza elimina ese directorio en un momento programado, un atacante puede aprovechar la ventana posterior para recrearlo con una estructura o contenido malicioso. La clave es que, más adelante, **snap-confine** vuelve a interactuar con esa ruta durante la inicialización del entorno y, si se cumplen las condiciones de carrera y permisos implicados, la cadena puede terminar derivando en ejecución con privilegios elevados.
- Mecanismo de falla: Un atacante con acceso local escalar privilegios hasta root en instalaciones por defecto de Ubuntu Desktop 24.04+ combinando snap-confine con la limpieza programada de systemd-tmpfiles. Aunque el ataque depende de una ventana temporal de limpieza (de 10 a 30 días según versión), el impacto final puede ser el control completo del equipo si no se actualiza snapd a versiones corregidas.
- Estado de explotación: No se han reportado ataques activos.

- Versiones afectadas: Ubuntu Desktop 24.04+

**Impacto potencial**

El fallo permite que un usuario local acabe ejecutando acciones como root, lo que en la práctica equivale a un compromiso total del sistema si el atacante ya ha conseguido una sesión en el equipo (por ejemplo, mediante credenciales robadas, una cuenta con pocos privilegios o acceso físico). La gravedad se califica como alta, con una puntuación CVSS 7.8 citada en el artículo.

**Recomendaciones de mitigación**

- La recomendación principal es actualizar snapd a una versión que ya incluya la corrección. Las versiones señaladas como solucionadas incluyen 2.73+ubuntu24.04.1 para Ubuntu 24.04, 2.73+ubuntu25.10.1 para Ubuntu 25.10, 2.74.1+ubuntu26.04.1 para Ubuntu 26.04 (rama de desarrollo, según el artículo) y, en el proyecto upstream, snapd 2.75 o superior. Para equipos gestionados en flota, conviene verificar la versión instalada y priorizar los sistemas Ubuntu Desktop 24.04+ donde el uso de Snaps es parte del flujo estándar. Como medida adicional de defensa, también resulta razonable vigilar comportamientos anómalos alrededor de /tmp/.snap, especialmente recreaciones inesperadas, cambios de propietario/permisos y patrones inusuales coincidiendo con ejecuciones de snap-confine o con tareas de limpieza de systemd-tmpfiles.
- Verifique si en su entorno está habilitado snapd:
  - systemctl status snapd
- Valide en qué versión se encuentra:
  - dpkg -l | grep snapd o apt list --installed | grep snapd
- En caso de requerir upgrade la versión de snapd puede ejecutar sudo apt update y luego sudo apt install snapd y verificar nuevamente.

**Ampliar información**

- https://unaaldia.hispasec.com/2026/03/cve-2026-3888-en-ubuntu-escalada-a-root-aprovechando-snap-confine-y-la-limpieza-de-systemd-tmpfiles.html?utm_source=rss&utm_medium=rss&utm_campaign=cve-2026-3888-en-ubuntu-escalada-a-root-aprovechando-snap-confine-y-la-limpieza-de-systemd-tmpfiles
- https://ubuntu.com/security/CVE-2026-3888
- https://www.cve.org/CVERecord?id=CVE-2026-3888

## GNU INETUTILS — EJECUCIÓN REMOTA DE CÓDIGO (RCE) NO AUTENTICADA EN TELNETD (CVE-2026-32746)

Se ha identificado una vulnerabilidad crítica en el demonio Telnet de GNU InetUtils que permite a un atacante remoto no autenticado ejecutar comandos arbitrarios con privilegios de superusuario. El fallo se manifiesta durante la fase de negociación inicial de la conexión, lo que permite el compromiso total del sistema antes de que se presente cualquier solicitud de credenciales o inicio de sesión.

**Resumen técnico:**

- Identificador principal: CVE-2026-32746.
- Severidad: 9.8 (Crítica) en la escala CVSS.
- Causa raíz: Escritura fuera de límites (buffer overflow) en el manejador de la subopción SLC (Set Local Characters) de LINEMODE.
- Mecanismo de falla: Un atacante puede desencadenar el desbordamiento enviando mensajes de protocolo especialmente diseñados al puerto 23/TCP durante el saludo inicial (handshake). Debido a que el demonio suele ejecutarse con privilegios elevados (vía inetd o xinetd), el exploit otorga control total de la máquina sin interacción del usuario.

- Estado de explotación: Crítico y sin parche oficial (esperado para abril del 2026). Alto riesgo debido a la explotación activa actual de fallos similares previos (CVE-2026-24061) según CISA.
- Versiones Afectadas: Sistemas Linux/Unix con la implementación de GNU InetUtils (telnetd) en todas las versiones hasta la 2.7 inclusive.

**Impacto potencial:**

- Control total del host: Obtención de una shell con privilegios de root, permitiendo la manipulación completa del sistema operativo.
- Ejecución de código pre-autenticación: Capacidad de comprometer el servidor de forma remota sin poseer un usuario o contraseña válidos.
- Persistencia y exfiltración: Instalación de puertas traseras (backdoors) persistentes y robo de información confidencial de la red.
- Movimiento lateral: Uso del sistema comprometido como punto de pivote para atacar otros dispositivos dentro de la infraestructura interna.

**Recomendaciones de mitigación:**

1. Deshabilitar el servicio Telnet: Se recomienda encarecidamente desactivar telnetd y migrar a protocolos de administración cifrados como SSH.
2. Restricción perimetral: Bloquear el acceso al puerto 23/TCP en firewalls perimetrales y locales, permitiendo únicamente conexiones desde hosts de confianza.
3. Ejecución sin privilegios: Si el uso de Telnet es indispensable, configurar el servicio para que se ejecute con un usuario sin privilegios administrativos (non-root).
4. Implementación de firmas IDS: Configurar sistemas de detección de intrusiones para alertar sobre subopciones SLC de LINEMODE con payloads inusualmente grandes (superiores a 90 bytes).

**Prioridad: Crítica.**

**Ampliar información:**

- https://cybersecuritynews.com/telnetd-vulnerability-enables-remote-attack/
- https://www.heise.de/en/news/Telnet-Critical-vulnerability-allows-injecting-malicious-code-from-the-network-11215681.html
- https://thehackernews.com/2026/03/critical-telnetd-flaw-cve-2026-32746.html
- https://abit.ee/en/cybersecurity/vulnerabilities/cve-2026-32746-telnetd-vulnerability-gnu-inetutils-root-rce-cybersecurity-port-23-en

## VULNERABILIDADES CRÍTICAS EN DISPOSITIVOS IP KVM (CVE-2026-32290 AL CVE-2026-32298)

Investigadores de seguridad han revelado la existencia de nueve vulnerabilidades críticas que afectan a dispositivos IP KVM (Keyboard, Video, Mouse over IP) de bajo costo. Estos fallos permiten a atacantes remotos no autenticados obtener acceso de nivel root y control total sobre los servidores y estaciones de trabajo conectados, operando por debajo de cualquier medida de seguridad del sistema operativo.

**Resumen técnico:**

- Identificadores: CVE-2026-32290 al CVE-2026-32298.
- Severidad: Hasta 9.8 (Crítica) en la escala CVSSv3.1.
- Causa raíz: Ausencia de validación de firmas en el firmware, falta de protección contra ataques de fuerza bruta, controles de acceso rotos e interfaces de depuración expuestas.

- Mecanismo de falla: Debido a que estos dispositivos emulan periféricos físicos (USB Gadgets), un atacante puede inyectar pulsaciones de teclas o simular unidades de almacenamiento para bootear sistemas operativos maliciosos, evadiendo cifrado de disco y Secure Boot.
- Estado de explotación: Descubrimiento reciente por investigadores de Eclypsium; existen exploits funcionales demostrados, aunque no se reporta explotación masiva "in the wild" hasta el momento.
- Versiones afectadas: Dispositivos IP KVM de los fabricantes GL-iNet (Comet RM-1), Angeet/Yeeso (ES3 KVM), Sipeed (NanoKVM) y JetKVM en diversas versiones de firmware.

**Impacto potencial:**

- Acceso a nivel de hardware: Control total del sistema host desde el BIOS/UEFI, permitiendo modificar configuraciones críticas antes de que cargue el sistema operativo o las soluciones de seguridad (EDR/AV).
- Persistencia indetectable: Capacidad de instalar implantes o backdoors directamente en el firmware del KVM, lo que permite la reinfección persistente del servidor incluso después de formatearlo.
- Inyección de comandos (BadUSB): Ejecución de scripts automáticos mediante la emulación de teclado, facilitando la exfiltración de datos o el despliegue de malware de forma silenciosa.
- Bypass de controles de red: Los atacantes pueden utilizar el KVM comprometido como un puente para saltar segmentaciones de red y acceder a segmentos de gestión altamente sensibles.

**Recomendaciones de mitigación:**

1. Aislamiento en Redes de Gestión (VLAN): Aislar estrictamente los dispositivos IP KVM en una VLAN de administración dedicada y prohibir cualquier acceso directo desde o hacia Internet.
2. Actualización de Firmware: Aplicar los parches disponibles de inmediato (especialmente JetKVM v0.5.4 y Sipeed NanoKVM v2.3.1); para los dispositivos sin parche (Angeet/Yeeso), considerar su desconexión inmediata.
3. Implementación de MFA y VPN: Forzar el uso de autenticación multifactor (MFA) para el acceso a la interfaz del KVM y requerir el uso de túneles VPN cifrados (como WireGuard o Tailscale) para cualquier acceso remoto.
4. Monitoreo de tráfico anómalo: Configurar alertas en sistemas de monitoreo de red para detectar conexiones salientes inesperadas desde los dispositivos KVM hacia direcciones IP externas desconocidas.

**Prioridad: Crítica.**

**Ampliar información:**

- https://www.govinfosecurity.com/cheap-dangerous-ip-kvms-carry-flaws-a-31054
- https://eclypsium.com/blog/your-kvm-is-the-weak-link-how-30-dollar-devices-can-own-your-entire-network/
- https://arstechnica.com/security/2026/03/researchers-disclose-vulnerabilities-in-ip-kvms-from-4-manufacturers/
- https://thehackernews.com/2026/03/9-critical-ip-kvm-flaws-enable.html

## MALWARE

### LEAKNET RANSOMWARE — CAMPAÑA DE ESCALAMIENTO MEDIANTE CLICKFIX Y LOADER DENO

El grupo de ransomware LeakNet (activo desde finales de 2024) ha evolucionado sus tácticas de acceso inicial, alejándose de los proveedores de credenciales robadas (IABs) para adoptar una agresiva campaña de ingeniería social denominada ClickFix. Esta operación destaca por el uso de un loader altamente sigiloso basado en el entorno de ejecución Deno, diseñado específicamente para evadir soluciones EDR mediante la ejecución de código directamente en la memoria del sistema.

**Resumen técnico:**

- Técnica principal: Ingeniería social avanzada mediante ClickFix y uso de loader basado en Deno.
- Vector de entrada: Sitios web legítimos comprometidos que presentan falsas verificaciones CAPTCHA (estilo Cloudflare Turnstile), induciendo al usuario a ejecutar un comando msiexec.exe fraudulento.
- Estrategia de evasión: Ejecución de payloads JavaScript/TypeScript codificados en Base64 directamente en memoria a través del ejecutable legítimo y firmado de Deno, minimizando artefactos forenses en disco.
- Mecanismo de control: Comunicación persistente con servidores de Comando y Control (C2) mediante protocolos WebSockets para recibir instrucciones y payloads de segunda etapa.

- Estado de la amenaza: Activa y en fase de escalamiento rápido (Marzo 2026), con un cambio estratégico que reduce la dependencia de proveedores de acceso inicial (IABs).

**Impacto potencial:**

- Cegado de la defensa (EDR Evasion): La ejecución en memoria mediante procesos de desarrollo legítimos permite que el ataque pase desapercibido ante motores de detección basados en firmas y análisis estático.
- Compromiso de identidades corporativas: Uso de herramientas nativas como klist para enumerar credenciales activas, permitiendo movimientos laterales inmediatos hacia servicios críticos sin solicitar nuevas contraseñas.
- Exfiltración masiva de activos: Uso de infraestructura de nube (buckets S3) para extraer datos sensibles, camuflando el tráfico de exfiltración bajo la apariencia de comunicaciones corporativas normales hacia la nube.
- Cifrado y secuestro de estaciones de trabajo: Una vez completada la fase de post-explotación (incluyendo DLL side-loading y movimiento lateral vía PsExec), el despliegue del ransomware resulta en el cifrado irreversible de los activos.

**Recomendaciones de mitigación:**

1. Restricción del diálogo "Ejecutar": Bloquear el acceso a la combinación de teclas Win+R y restringir la ejecución de comandos msiexec desde navegadores web mediante políticas de grupo (GPO).
2. Monitoreo de Runtimes externos: Implementar reglas de detección para identificar la presencia y ejecución del binario deno.exe fuera de entornos de desarrollo autorizados, especialmente en rutas como C:\ProgramData\.
3. Auditoría de persistencia en disco: Vigilar la creación inusual de servicios y el DLL side-loading (ej. jli.dll) en directorios compartidos del sistema como \USOShared\.

4. Control de tráfico hacia nubes públicas: Restringir el tráfico saliente hacia buckets S3 que no pertenezcan a la organización y bloquear la resolución de dominios con una antigüedad menor a 30 días.

**Prioridad: Urgente.**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/leaknet-ransomware-uses-clickfix-and-deno-runtime-for-stealthy-attacks/
- https://ciberblog.net/noticias/leaknet-ransomware-clickfix-deno-loader
- https://thehackernews.com/2026/03/leaknet-ransomware-uses-clickfix-via.html
- https://cybersecuritynews.com/leaknet-scales-ransomware-operations/#google_vignette

**Recomendaciones generales sobre malware:**

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

## NOTICIAS DE CIBERSEGURIDAD

### SHADOW AI — EL RIESGO INVISIBLE DEL USO NO CONTROLADO DE INTELIGENCIA ARTIFICIAL EN LAS EMPRESAS

El fenómeno del Shadow AI (o "IA en la sombra") se ha convertido en una de las mayores preocupaciones para los departamentos de TI y Seguridad en 2026. Recientes informes indican que el 68% de los colaboradores utiliza herramientas de IA generativa (como ChatGPT, Claude o frameworks como OpenClaw) en sus flujos de trabajo profesionales sin la aprobación o supervisión de la organización. Esta práctica, motivada por la búsqueda de productividad, está abriendo brechas críticas de seguridad y cumplimiento normativo en infraestructuras corporativas.

**Resumen técnico:**

- Alcance: Afecta al 68% de los empleados en promedio, alcanzando el 82% en el sector tecnológico.
- Impacto principal: Fuga involuntaria de datos corporativos, propiedad intelectual y código fuente hacia modelos públicos de entrenamiento.
- Estadísticas clave: El 44% de los usuarios emplea las mismas herramientas de IA tanto para fines personales como profesionales.
- Estado de la tendencia: En crecimiento acelerado; el uso de agentes autónomos (SaaS Shadow AI) ha provocado un incremento del 490% en ataques a aplicaciones SaaS año tras año.

**Impacto potencial:**

- Pérdida de confidencialidad: Exposición de datos críticos del negocio que son absorbidos por los algoritmos de IA para el aprendizaje continuo de terceros.
- Incumplimiento normativo: Riesgo de violaciones al RGPD y otras leyes de privacidad, con multas potenciales de hasta el 4% de la facturación anual.
- Explotación de agentes (Agentic AI): El uso de frameworks como OpenClaw sin supervisión permite a los atacantes secuestrar agentes de IA para ejecutar comandos locales y moverse lateralmente en la red.
- Sesgo y desinformación: Toma de decisiones críticas (finanzas, RR.HH.) basadas en modelos no validados que pueden contener prejuicios o información errónea.

**Recomendaciones para mitigar el riesgo:**

1. Establecer marcos de gobernanza: Definir políticas claras de uso de IA y designar responsables (Chief AI Officers) para supervisar la adopción tecnológica.
2. Implementar Sandboxes seguros: Proporcionar entornos controlados e instancias privadas de IA para que los empleados experimenten sin exponer datos corporativos.
3. Monitoreo y DLP: Reforzar las soluciones de prevención de pérdida de datos para identificar el envío de información sensible hacia plataformas de IA públicas.
4. Formación y Sensibilización: Capacitar a los empleados sobre los riesgos de privacidad y seguridad asociados al uso de "prompts" con información real de la empresa.

**Prioridad: Importante.**

**Ampliar Información:**

- https://www.forbes.com/councils/forbestechcouncil/2026/03/16/why-ai-is-about-to-make-shadow-it-look-like-a-minor-problem/
- https://www.securityweek.com/the-shadow-ai-problem-how-saas-apps-are-quietly-enabling-massive-breaches/
- https://blog.grupomicronet.com/openclaw-el-nuevo-riesgo-de-shadow-ai-que-amenaza-a-las-redes-empresariales
- https://blog.segu-info.com.ar/2026/03/shadow-ia-cuando-la-inteligencia.html