La vulnerabilidad **CVE-2025-29824** representa una grave falla de seguridad en el componente CLFS (Common Log File System) de los sistemas Windows, específicamente relacionada con una condición de "uso después de liberación" (Use-After-Free). Esta condición ocurre cuando un área de memoria es liberada pero luego accedida nuevamente, lo que abre la puerta para que un atacante manipule esa memoria y ejecute código arbitrario.

El vector de ataque comienza con un acceso local y limitado: un atacante ya presente en el sistema, incluso con privilegios bajos (como un usuario estándar), puede aprovechar esta falla para escalar sus privilegios hasta obtener control total del sistema operativo a nivel SYSTEM, el nivel más alto de autoridad en Windows.

Este tipo de vulnerabilidad es especialmente peligrosa porque no requiere conexión remota ni explotación a través de la red; se activa desde dentro del sistema, lo que la hace muy atractiva para operadores de ransomware y actores de amenazas persistentes (APT) que ya lograron un punto de entrada y buscan afianzarse.

Lo alarmante es que ha sido utilizada activamente en campañas reales de ataques, permitiendo el despliegue de ransomware altamente destructivo, a menudo después de una fase inicial de reconocimiento sigiloso y movimiento lateral dentro de la red.

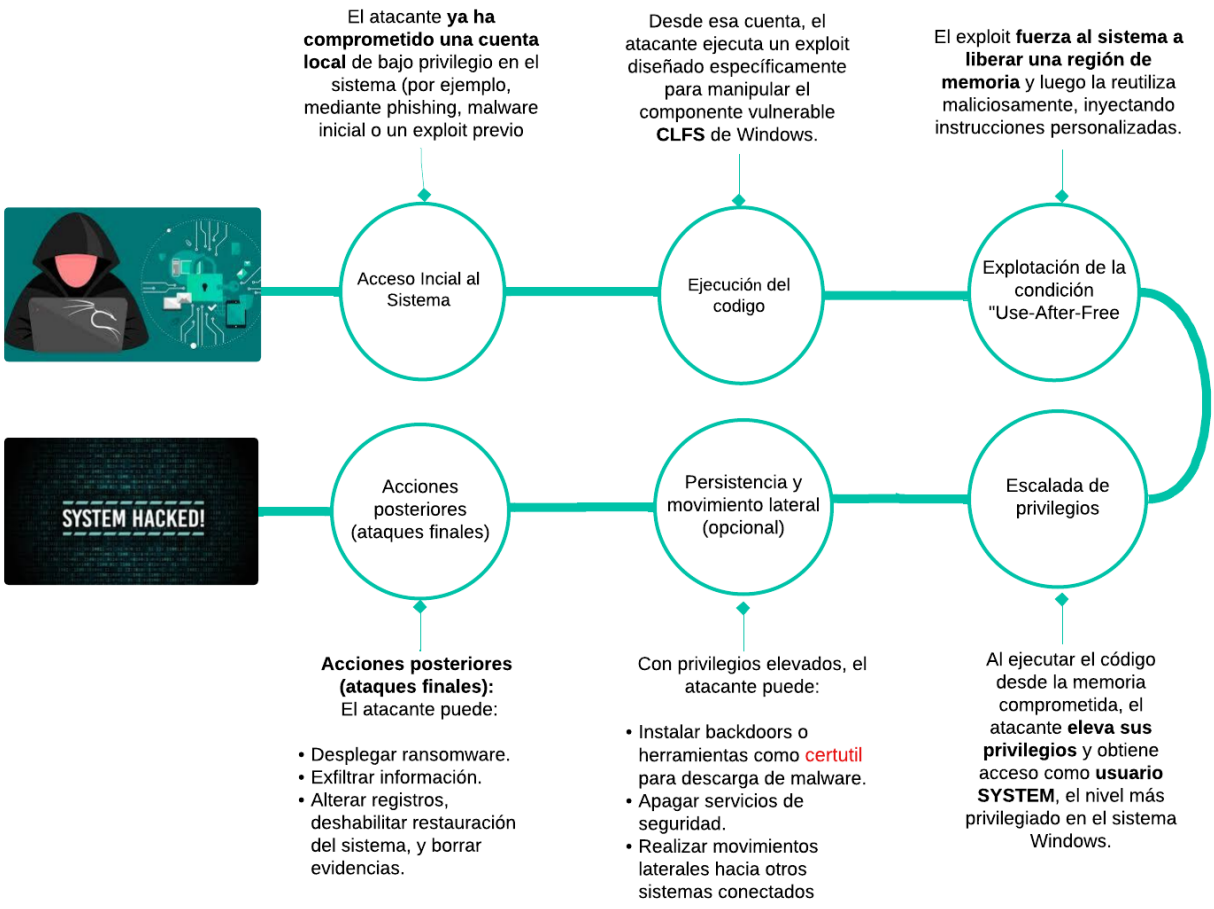
Storm-2460, una agrupación cibercriminal vinculada a actividades de ransomware. El grupo aprovechó la vulnerabilidad **CVE-2025-29824** en entornos Windows mediante un exploit que les permitió escalar privilegios localmente.
Tras lograr acceso como **SYSTEM**, desplegaron su carga maliciosa mediante un **binario llamado PipeMagic**, una herramienta personalizada para distribuir ransomware.
Organizaciones afectadas en los sectores de tecnología, bienes raíces, salud, y comercio al por menor, principalmente en EE. UU. y Europa.

https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

www.csirtsalud.gov.co

Vector de ataque:



Impactos y riesgos:

Impacto	Riesgo
Compromiso total del sistema	La explotación exitosa permite al atacante obtener control total del sistema, facilitando acciones como la instalación de Malware, modificación de configuraciones críticas y acceso a datos sensibles.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

www.csirtsalud.gov.co

Impacto	Riesgo
Despliegue de ransomware	Se ha observado que grupos de amenazas, como Storm-2460, han explotado esta vulnerabilidad para desplegar ransomware utilizando el malware PipeMagic, afectando sectores como tecnología, bienes raíces, finanzas y retail en diversas regiones.
Persistencia y evasión	Los atacantes pueden utilizar herramientas legítimas del sistema, como *certutil*, para descargar cargas maliciosas, y emplear técnicas para borrar registros de eventos y deshabilitar opciones de recuperación, dificultando la detección y respuesta.

Recomendaciones:

- ✓ Aplicar parches de seguridad recomendados por el proveedor, Microsoft ha lanzado actualizaciones para corregir esta vulnerabilidad en su boletín de seguridad de abril de 2025. Es imperativo aplicar estos parches en todos los sistemas afectados.
- ✓ Realizar la actualización a versiones de Windows no afectadas, como Windows 11 versión 24H2, que no son susceptibles a esta explotación específica.
- ✓ Activar la protección basada en la nube en soluciones antivirus para detectar y bloquear amenazas emergentes.
- ✓ Utilizar soluciones de detección y respuesta en endpoints (EDR) en modo de bloqueo para prevenir la ejecución de artefactos maliciosos.
- ✓ Habilitar el registro detallado de eventos y monitorear actividades sospechosas, como el uso inusual de certutil o la ejecución de scripts de MSBuild no autorizados.
- ✓ Revisar regularmente los registros de eventos para detectar signos de explotación o actividades anómalas.
- ✓ Educar a los usuarios sobre las prácticas de seguridad, incluyendo la precaución al descargar y ejecutar archivos de fuentes no verificadas, y la importancia de reportar comportamientos inusuales en sus sistemas

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570
www.csirtsalud.gov.co

Fuentes:

- https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/
- https://nvd.nist.gov/vuln/detail/CVE-2025-29824
- https://www.bleepingcomputer.com/news/security/microsoft-windows-clfs-zero-day-exploited-by-ransomware-gang/
- https://www.linkedin.com/pulse/explotaci%C3%B3n-activa-de-la-vulnerabilidad-cve-2025-29824-cbb6e/

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

www.csirtsalud.gov.co