Alerta

Técnica

Vulnerabilidad explotada en Windows

COLCERT AL-20251009-079

TLP:CLEAR

Se ha identificado la **explotación activa** de la vulnerabilidad **CVE-2021-43226** en el componente **Common Log File System (CLFS)** de **Microsoft Windows**, la cual permite la escalación de privilegios locales hasta nivel SYSTEM. Esta condición, actualmente incluida por CISA en el catálogo de vulnerabilidades explotadas (KEV), representa un riesgo elevado de movimientos laterales y persistencia en entornos corporativos comprometidos.

Aunque su uso en campañas de *ransomware* aún es incierto, la probabilidad de adopción por actores de amenaza en los próximos meses es alta, dada la recurrencia de fallos similares en operaciones recientes. La anticipación y priorización de parches, junto con controles de integridad y monitoreo de anomalías en drivers del *kernel*, se vuelven esenciales para reducir la incertidumbre operacional y el riesgo estratégico ante posibles explotaciones futuras.

NIVEL DE RIESGO

ALTO

Vulnerabilidad identificada

CVE	PRODUCTOS AFECTADOS	SCORE CVSS	DESCRIPCIÓN	CISA KEV
CVE-2021-43226	Microsoft Windows 10, Windows 11, Windows Server 2016, 2019 y 2022 (componentes que utilizan el driver Common Log File System – CLFS).	**7.8 (Alta)**	Vulnerabilidad de **escalación de privilegios locales** en el componente Common Log File System (CLFS) de Windows. Un atacante autenticado podría aprovechar un manejo inadecuado de los objetos en memoria del driver *clfs.sys* para ejecutar código arbitrario con privilegios SYSTEM, permitiendo el control total del equipo afectado.	**TRUE**

¿Cómo se podrían explotar esta debilidad?

Prerrequisito de acceso local y autenticado: el ciberdelincuente primero obtiene acceso al sistema con una cuenta local o credenciales de usuario (por ejemplo, tras un phishing, credenciales capturadas o movimiento lateral). La vulnerabilidad en CLFS requiere interacción local. No es un vector de ejecución remota por sí sola.

Identificación del objetivo vulnerable: el actor de amenaza identifica sistemas con versiones de Windows que cargan el driver *clfs.sys* vulnerable (equivalente a verificar disponibilidad del componente CLFS y nivel de parche).

Engaño de validaciones del *driver*: aprovechando una falla en la validación del manejo de objetos y estructuras internas del *driver* CLFS, el atacante provoca condiciones (por ejemplo, referencias inválidas, race conditions o manejo inadecuado de buffers) que permiten leer o escribir memoria del kernel o corromper estructuras de control.

Obtención de capacidades elevadas: la manipulación del kernel se usa para sobrescribir funciones, punteros o credenciales en memoria, de modo que el proceso malicioso o una nueva *shell* se ejecuten con privilegios SYSTEM. Esto proporciona control total sobre el host afectado.

Despliegue de *malware* y consolidación de acceso: con privilegios elevados, el atacante instala herramientas persistentes (*backdoor*, *loader*, herramientas de administración remota), crea cuentas y/o servicios con privilegios, o modifica políticas para evadir controles.

Movimientos laterales y objetivos finales: la escalación a SYSTEM facilita la exfiltración de credenciales, acceso a controladores de dominio, cifrado masivo (*ransomware*), o sabotaje. A menudo es usada como eslabón en cadenas más largas de intrusión post-explotación.

Evasión y remoción de trazas: el cibercriminal intenta limpiar registros, manipular logs o usar herramientas legítimas del sistema para ocultar acciones (*living-off-the-land*), complicando la detección forense.

Impacto para Colombia y la región

- **Sectores afectados**: gobierno, salud, financiero, energía, TIC, educación, transporte, comercio, industria y turismo.

- **Riesgo alto**: la vulnerabilidad permite escalación local a SYSTEM, facilitando movimientos laterales y consolidación de control en equipos ya comprometidos. Además CISA la ha incluido en su catálogo de “Known Exploited Vulnerabilities”, lo que eleva la probabilidad de adopción por actores de amenazas.

- **Posibles consecuencias**
  - Compromiso y pérdida de control de servidores y endpoints críticos.
  - Facilitación de ataques de *ransomware* y extorsión por acceso privilegiado.
  - Exfiltración de información sensible (datos personales, financieros o de salud).
  - Interrupción de servicios esenciales (energía, atención médica, transacciones financieras).
  - Costos operacionales y reputacionales significativos, multas por incumplimiento de protección de datos.

- **Implicaciones en seguridad digital**
  - Necesidad de priorizar parches y validación de cumplimiento en infraestructuras críticas y proveedores.
  - Refuerzo de la detección de anomalías a nivel kernel y monitoreo centralizado (SIEM/EDR) para identificar escalaciones locales.
  - Revisión de controles de acceso local, segmentación de red y políticas de ejecución.
  - Preparación de equipos de respuesta para contención rápida, análisis forense y recuperación (imágenes limpias, rescate de backups).

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación para escalamiento de privilegios	**T1068**	Aprovechamiento de una vulnerabilidad de *software* (incluyendo en el kernel o drivers) para ejecutar código controlado por el atacante y elevar privilegios en el sistema. Encaja directamente con exploits sobre clfs.sys que permiten llegar a SYSTEM.
Secuestro del flujo de ejecución (Hijack Execution Flow)	**T1574**	Técnicas que permiten a un adversario alterar la forma en que se ejecutan programas con fines de persistencia, evasión o elevación de privilegios. Incluye subtécnicas aplicables a *drivers* y *callbacks*.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Abuso de mecanismos de elevación (Abuse Elevation Control Mechanism)	**T1548**	Aprovechar mecanismos nativos de control de elevación o sus configuraciones para obtener permisos más altos. Relevante como alternativa a *exploits* de kernel cuando el adversario busca elevar privilegios.
Inyección en procesos (Process Injection)	**T1055**	Ejecutar código dentro del espacio de direcciones de otro proceso legítimo para ocultar actividad, moverse con los privilegios del proceso objetivo y, potencialmente, alcanzar capacidades elevadas tras explotación. Frecuente en fases post-explotación
Explotación para escalamiento de privilegios	**T1068**	El adversario aprovecha vulnerabilidades en software o componentes del sistema para ejecutar código que le permita obtener privilegios más altos (p. ej. cuenta SYSTEM o root), facilitando control administrativo y movimiento lateral.
Inyección en procesos	**T1055**	Inserción o ejecución de código malicioso dentro de procesos legítimos para evadir detección, ocultar actividad y mantener persistencia en el sistema.
Abuso de mecanismos de control de elevación	**T1548**	Uso indebido de mecanismos de control de elevación de privilegios (por ejemplo UAC en Windows u otros mecanismos de control de acceso) para ejecutar acciones o comandos con privilegios elevados sin autorización.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Actualizar software (Update Software)	**M1051**	Aplicar parches de sistema operativo, *drivers* y *firmware* reduce directamente la exposición a *exploits* que aprovechan vulnerabilidades del kernel como clfs.sys. Es la medida primaria y prioritaria para eliminar la ventana de explotación.
Protección contra exploits (Exploit Protection)	**M1050**	Tecnologías de protección dificultan la explotación de vulnerabilidades en memoria y pueden bloquear o detectar intentos de escalamiento por CVE-2021-43226. Relevante como control compensatorio hasta aplicar parches.
Integridad de procesos privilegiados (Privileged Process Integrity)	**M1025**	Asegurar que procesos y servicios privilegiados (y sus drivers asociados) no puedan ser inyectados, esto limita la posibilidad de que un *exploit* de kernel o flujo de ejecución secuestrado consolide privilegios SYSTEM. Ayuda a mitigar técnicas de *hijack* e inyección de procesos.
Aislamiento y sandboxing de aplicaciones (Application Isolation and Sandboxing)	**M1048**	Ejecutar componentes en entornos aislados o restringidos (o aplicar controles de ejecución) reduce el impacto de una explotación local, limitando el acceso a recursos sensibles y frenando movimientos laterales post-explotación. Útil como medida adicional de contención.

Soluciones y mitigaciones disponibles

- ❑ **Implementar de inmediato las actualizaciones de seguridad publicadas por Microsoft para corregir CVE-2021-43226** (disponibles vía Windows Update y Microsoft Update Catalog, referenciadas en la guía de actualizaciones de seguridad de Microsoft) y confirmar el número del KB (Knowledge Base) correspondiente al parche oficial consultando la Security Update Guide o el catálogo de actualizaciones.
- ❑ **Reforzar las políticas de control de privilegios** para restringir la ejecución de procesos con privilegios elevados, aplicando el principio de mínimo privilegio y evitando que usuarios locales o servicios no autorizados accedan a funciones del kernel.
- ❑ Habilitar las funciones de protección contra *exploits* integradas en el sistema operativo, tales como **Exploit Protection, Kernel Control Flow Guard** (CFG) y **Memory Integrity** (HVCI), con el fin de reducir las posibilidades de ejecución arbitraria de código.
- ❑ **Monitorear los eventos del sistema en busca de comportamientos anómalos** o escalamiento de privilegios inusuales, especialmente aquellos asociados al archivo clfs.sys, utilizando herramientas EDR o SIEM.
- ❑ **Fortalecer la segmentación de red y los controles de acceso** para evitar que un atacante con acceso local pueda desplazarse lateralmente hacia otros sistemas de la red.
- ❑ **Implementar controles de integridad y firma de controladores**, asegurando que sólo los binarios firmados y verificados por Microsoft puedan cargarse en el entorno del sistema operativo.
- ❑ **Documentar la aplicación de los parches** y establecer un **proceso de gestión continua de vulnerabilidades**, priorizando las que impactan directamente la escalación de privilegios locales en entornos Windows.
- ❑ Activar políticas de control de aplicaciones (AppLocker o Windows Defender Application Control – WDAC) para restringir la ejecución de archivos y scripts no autorizados en el sistema operativo. Esta medida previene que atacantes con acceso local ejecuten binarios maliciosos o herramientas no firmadas que puedan aprovechar vulnerabilidades del kernel.

Fuentes

CISA (Cybersecurity & Infrastructure Security Agency), 09/11/2021 – CVE-2021-43226 – Catalog of Known Exploited Vulnerabilities (KEV), disponible en:
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Microsoft, 09/11/2021, CVE-2021-43226 – Windows Common Log File System Driver Elevation of Privilege Vulnerability, Fuente oficial del proveedor.
https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-43226
Cybersecurity News, 07/10/2025, CISA adds Windows Privilege Escalation Vulnerability to KEV Catalog, Fuente de ciberseguridad especializada. https://cybersecuritynews.com/cisa-windows-privilege-escalation-vulnerability/
CVE.org, 09/11/2021, CVE-2021-43226 Detail, Base de datos oficial de vulnerabilidades.
https://www.cve.org/CVERecord?id=CVE-2021-43226
NIST NVD (National Vulnerability Database), 09/11/2021, CVE-2021-43226 Detail – Windows Common Log File System Driver Elevation of Privilege Vulnerability, Fuente gubernamental de referencia técnica.
https://nvd.nist.gov/vuln/detail/CVE-2021-43226