Boletín informativo vulnerabilidad Windows Escalamiento de privilegios

CSIRTSALUD-AL-20251010-42 **TLP: CLEAR**

Incidente ID:	42
Fecha del reporte:	10/10/2025
Entidad:	Entidades del ecosistema Digital
Título:	Vulnerabilidad de escalamiento de privilegios locales Microsoft Windows
Herramienta de detección	N/A
Activo involucrado:	Sistema Operativo Microsoft Windows
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las Entidades del ecosistema Digital sobre la vulnerabilidad de explotación activa identificada como CVE-2021-43226 que afecta el componente Common Log File System (CLFS) en las versiones de Microsoft Windows.

Descripción:

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 a un atacante poder realizar un escalamiento de privilegios locales hasta nivel de usuario SYSTEM. Actualmente esta vulnerabilidad se encuentra incluida en el catálogo de vulnerabilidades explotadas (KEV), publicadas por CISA con un riesgo elevado de movimientos laterales y persistencia en las Entidades comprometidas.

Un atacante con una autenticación 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 lo que representaría un riesgo alto para las Entidades.

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

Productos afectados de Microsoft:

- Microsoft Windows 10 (versión con fin de soporte 14 de octubre 2025)
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Componentes de Microsoft que utilizan driver Common Log File System – CLFS

Como se podría explotar esta vulnerabilidad

- Acceso local y autenticado: la vulnerabilidad solo se puede explotar con un acceso local y autenticado en el sistema de la Entidad.
- Engaño de validaciones de driver: aprovechando una falla en la validación del manejo de objetos y estructuras internas del driver CLFS, se provocarían condiciones de referencias inválidas, race conditions o manejo inadecuado de buffers.
- 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 equipo de la Entidad afectado.
- Despliegue de malware y consolidación de acceso: con privilegios elevados, se instalarían herramientas persistentes como puertas traseras, loader, herramientas de administración remota tales como teamviewer, anydesk para la creación de cuentas y/o servicios con privilegios o modificar alguna política para lograr evadir controles.
- Movimientos laterales y objetivos finales: el escalamiento a un usuario SYSTEM facilita la exfiltración de credenciales, acceso a controladores de dominio, cifrado masivo (ransomware), o sabotaje

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

Sectores afectados

Gobierno, salud, financiero, energía, TIC, educación, transporte, comercio, industria y turismo

Técnicas MITRE ATT&CK Detectadas:

MITRE ATT&CK	Técnicas Claves
T1548	Abuso de mecanismos de elevación (Abuse Elevation Control Mechanism)
T1055	Inyección en procesos (Process Injection)
T1068	Explotación para escalamiento de privilegios
T1055	Inyección en procesos
T1548	Abuso de mecanismos de control de elevación

Recomendaciones de mitigación:

- Implementar de inmediato las actualizaciones de seguridad publicadas por Microsoft para corregir CVE2021-43226 disponibles en Windows Update y Microsoft update Catalog
- Reforzar políticas de control de privilegios para restringir a ejecución de procesos con privilegios elevados, aplicando el principio de mínimo privilegio.
- 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).
- 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.

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

- 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

Fuentes:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-43226
- https://cybersecuritynews.com/cisa-windows-privilege-escalation-vulnerability/
- https://www.cve.org/CVERecord?id=CVE-2021-43226
- https://nvd.nist.gov/vuln/detail/CVE-2021-43226

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

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