Incidente ID:	0019
Fecha del reporte:	18/12/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad Desktop Windows Manager
Herramienta de detección	N/A
Activo involucrado:	Microsoft Windows
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad con código CVE-2025-55681 que esta afectando los entornos de Windows, es una vulnerabilidad de nivel Alta de límites en el Administrador de Ventanas de Escritorio (DWM) que permite a atacantes locales escalar privilegios a SISTEMA en los sistemas Windows afectados

Descripción:

Microsoft ha confirmado una vulnerabilidad crítica de desbordamiento de límites en el Desktop Window Manager (DWM) que permite a atacantes locales escalar privilegios a SYSTEM en los sistemas Windows afectados.

La vulnerabilidad, identificada como CVE-2025-55681, reside en el componente dwmcore.dll, un componente crítico responsable de renderizar efectos visuales y gestionar operaciones gráficas.

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

Los atacantes que obtengan acceso local a un sistema afectado pueden explotar un manejo incorrecto del buffer para ejecutar código con privilegios elevados.

La vulnerabilidad no requiere interacción del usuario una vez que se obtiene el acceso inicial al sistema. Lo que la hace particularmente peligrosa en entornos empresariales donde múltiples usuarios comparten sistemas o donde se implementan soluciones de acceso remoto.

La vulnerabilidad tiene una puntuación CVSS v3.1 de 7.8, lo que indica una severidad alta. Un atacante autenticado con privilegios de usuario de bajo nivel puede eludir los controles de seguridad y obtener acceso irrestricto al sistema.

Productos afectados:

La vulnerabilidad afecta a una amplia gama de sistemas operativos Microsoft Windows, incluyendo:

Producto	Versiones Afectadas
Windows 11	Versiones 22H2, 23H2, 24H2 y 25H2
Windows 10	Versiones 22H2, 21H2 y 1809 (LTSC)
Windows Server	2019, 2022 y 2025 (incluyendo Server Core)

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

Modo de explotación y cadena de infección

Los adversarios utilizan las siguientes tácticas y técnicas para aprovechar este fallo:

- T1068 - Exploitation for Privilege Escalation: Uso del exploit para obtener permisos de administrador.
- T1574.002 - DLL Side-Loading: Carga de bibliotecas maliciosas para ejecutar código en procesos legítimos.
- T1548.002 - Abuse Elevation Control Mechanism (UAC Bypass): Evasión de las alertas de confirmación de Windows para ganar privilegios.

El vector de ataque es Local (AV:L), lo que significa que el atacante ya debe tener una sesión en la máquina o haber logrado ejecutar código inicial mediante otro método (como un malware previo). El flujo de explotación documentado es el siguiente:

- Se desencadena el error de lectura fuera de límites para ejecutar shellcode inicial.
- Se realiza un "hook" a la función MapViewOfFile para manipular la memoria compartida.
- Se interfiere con el proceso consent.exe (encargado de las solicitudes de Control de Cuentas de Usuario - UAC).
- Finalmente, se fuerza la carga de una librería (DLL) que ejecuta una consola de comandos (cmd.exe) con privilegios de SYSTEM.

Indicadores de Compromiso (IoCs)

Dado que es una explotación local, los administradores deben buscar:

- Procesos sospechosos: Instancias de cmd.exe o powershell.exe cuyo proceso padre sea consent.exe o dwm.exe.

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

- Carga de DLLs no firmadas: Monitoreo de carga de librerías inusuales en la ruta de ejecución de los servicios de escritorio.
- Logs de Eventos: Presencia frecuente de errores o caídas del proceso dwm.exe justo antes de una elevación de privilegios.
- Actividad de Memoria: Anomalías en el uso de memoria compartida por parte de usuarios con bajos privilegios.

Recomendaciones de mitigación:

- Aplicar Parches Inmediatamente: Instalar las actualizaciones acumulativas de Windows correspondientes al mes de octubre de 2025 o posteriores.

- Verificación de Versión: Asegurar que el sistema ha superado los números de compilación corregidos:

Sistema Operativo	Versión / Canal	Compilación Comprometida (Vulnerable)	Compilación Segura (Parche Aplicado)
Windows 11	24H2 / 25H2	Menor o igual a 10.0.26100.6898	10.0.26100.6899 o superior
Windows 11	23H2 / 22H2	Menor o igual a 10.0.22631.6059	10.0.22631.6060 o superior
Windows 10	22H2 / 21H2	Menor o igual a 10.0.19045.6455	10.0.19045.6456 o superior
Windows 10	1809 (LTSC)	Menor o igual a 10.0.17763.7918	10.0.17763.7919 o superior
Windows Server	2025	Menor o igual a 10.0.26100.6898	10.0.26100.6899 o superior
Windows Server	2022	Menor o igual a 10.0.20348.4293	10.0.20348.4294 o superior
Windows Server	2019	Menor o igual a 10.0.17763.7918	10.0.17763.7919 o superior

- Principio de Menor Privilegio: Restringir el acceso local a servidores críticos y monitorear sesiones de usuario inusuales.

- Uso de EDR/Antivirus: Asegurar que las soluciones de detección de puntos finales (EDR) estén configuradas para detectar técnicas de inyección de código y "hooking" de memoria.

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

Fuentes:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55681
- https://blog.elhacker.net/2025/12/vulnerabilidad-dwm-windows.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-desktop-window-manager-de-windows-permite-escalada-de-privilegios/
- https://www.cve.org/CVERecord?id=CVE-2025-55681
- https://cybersecuritynews.com/microsoft-desktop-windows-manager-vulnerability/

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