Boletín informativo
Vulnerabilidad en Windows Admin Center

CSIRTSALUD-AV-20260218-29 **TLP: AMBER**

Alerta ID:	0029
Fecha del reporte:	18/02/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en Windows Admin Center
Herramienta de detección	N/A
Activo involucrado:	Windows Admin Center
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Crítico

Resumen ejecutivo

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad crítica **CVE-2026-26119** que afecta a **Windows Admin Center**. Este documento busca proporcionar los detalles técnicos necesarios para comprender el riesgo, identificar posibles intentos de explotación y aplicar las medidas de mitigación urgentes publicadas por Microsoft el 17 de febrero de 2026.

Descripción:

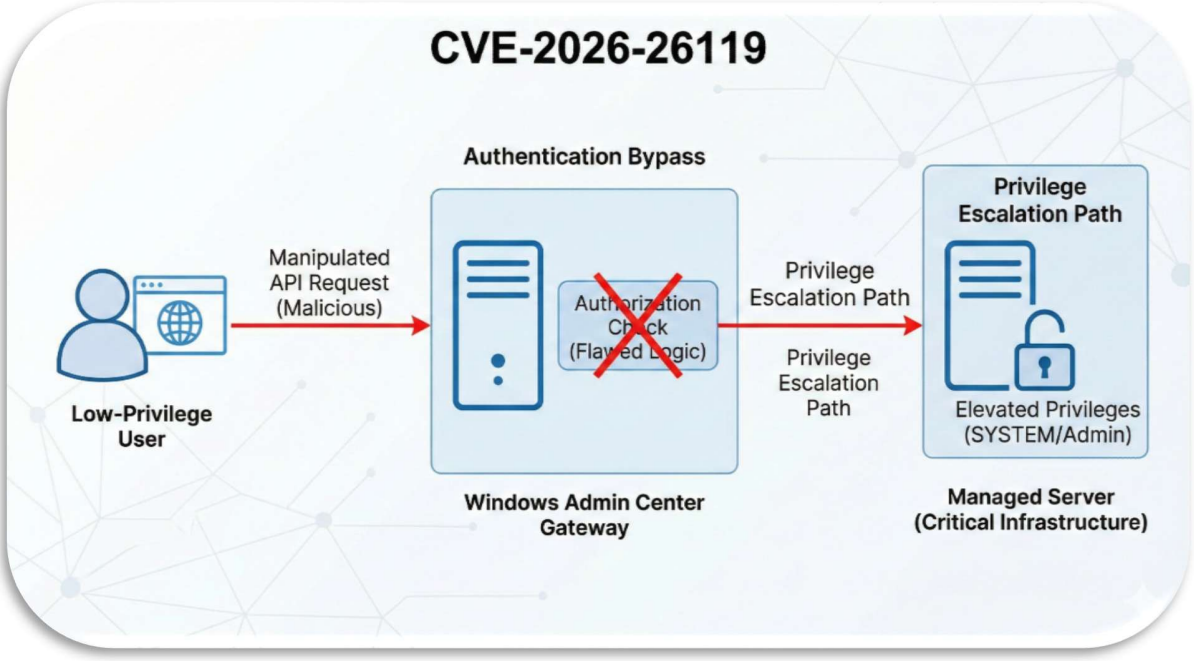
La falla, calificada como **CVSS 8.8 (crítica)**, se debe a una autenticación incorrecta **(CWE-287)** que podría permitir que un atacante autorizado obtenga privilegios de red elevados. Windows Admin Center no valida correctamente ciertas solicitudes de red, lo que permite que un atacante que ya cuenta con credenciales de nivel bajo (usuario autorizado) eluda los controles de seguridad.

A diferencia de un ataque de fuerza bruta, aquí el sistema "confía" erróneamente en la identidad o los permisos del atacante debido a una falla en la lógica de verificación de la sesión. Esto

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

permite que una cuenta con acceso limitado realice acciones administrativas completas en los servidores gestionados.

Aunque Microsoft no ha observado una explotación activa en la naturaleza, advierte que la explotación es "más probable", citando la baja complejidad del ataque y la **exposición de la red de las implementaciones de WAC.**



Modo de explotación y cadena de infección

La vulnerabilidad **CVE-2026-26119** reside en la lógica de validación de **autenticación y autorización (RBAC)** dentro del *Gateway* de Windows Admin Center. El flujo de ataque se desarrolla en las siguientes fases:

- **Pre-requisito de Acceso (Valid Accounts):** El atacante debe contar con una identidad válida en el dominio o en el sistema local, aunque sea con privilegios mínimos (ej. un usuario del grupo "Domain Users" o una cuenta de servicio comprometida con acceso de "solo lectura" al panel).

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

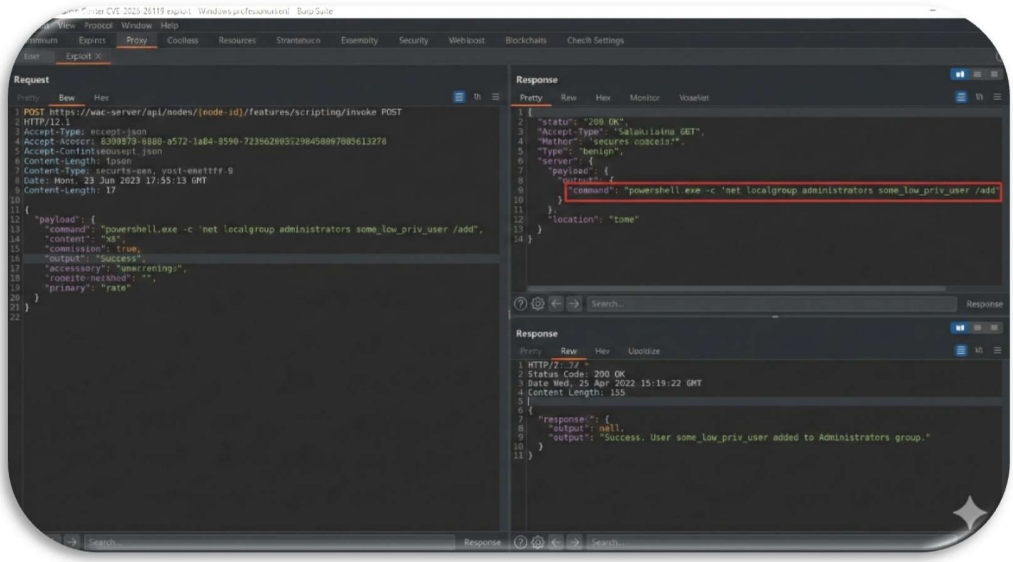
- **Manipulación de Solicitudes API (API Abuse):** Windows Admin Center actúa como una pasarela que traduce las acciones de la interfaz web a comandos de PowerShell/WMI ejecutados sobre **WinRM** en los nodos gestionados.

  - El atacante intercepta la comunicación entre su navegador y el *Gateway* del Admin Center.
  - Se identifica una solicitud HTTP (o mensaje WebSocket) específica encargada de funciones administrativas críticas (ej. creación de usuarios, ejecución de scripts).
  - Debido a una **validación de entrada impropia**, el atacante puede modificar el *payload* de la solicitud o los encabezados de sesión.

- **Elusión de Controles (Authorization Bypass):** El componente backend del Admin Center falla al re-verificar los permisos del usuario *antes* de procesar la solicitud manipulada. El sistema asume erróneamente que la solicitud es legítima basándose en la sesión activa inicial, sin validar si ese usuario específico tiene permisos para la *acción* específica solicitada.

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

- **Ejecución con Privilegios Elevados:** El *Gateway* procesa la orden y la envía al servidor objetivo utilizando la **Delegación de Credenciales** o la cuenta de servicio del propio Admin Center (que a menudo corre con altos privilegios o *NT AUTHORITY\SYSTEM*).



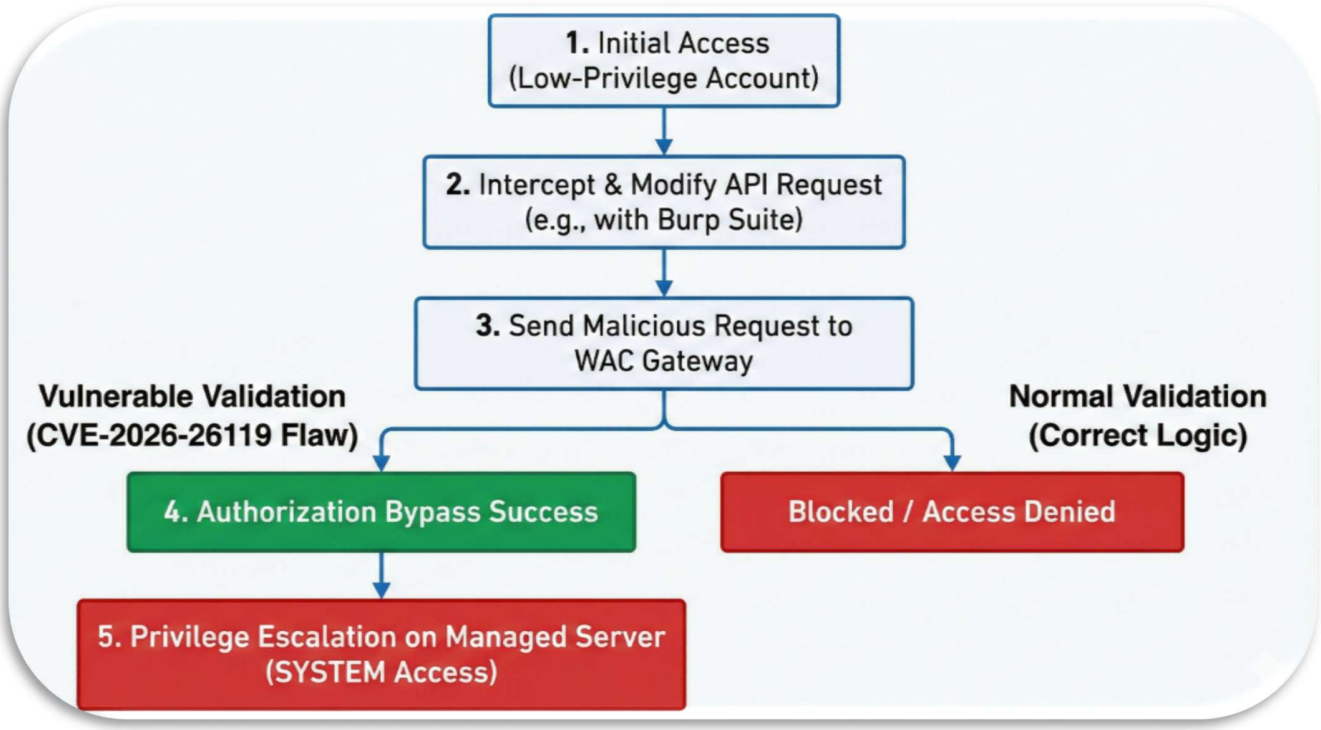
El código arbitrario o el comando administrativo se ejecuta en el servidor destino con permisos de *SYSTEM* o *Administrador*, completando la escalada de privilegios vertical.

Al entender que es una **manipulación de API**, se entiende que la detección no debe buscar solo "intentos de login fallidos", sino **sesiones de usuarios con bajos privilegios que generan tráfico hacia endpoints de administración (URI/API endpoints)** que normalmente solo tocarían los administradores globales.

Este ataque se alinea principalmente con la táctica de **Escalada de Privilegios (Privilege Escalation)**.

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

Táctica	ID Técnica	Nombre de la Técnica	Descripción
Privilege Escalation	**T1068**	*Exploitation for Privilege Escalation*	El adversario explota una debilidad en el software (Windows Admin Center) para ganar privilegios superiores a los que tenía.
Initial Access	**T1078**	*Valid Accounts*	El ataque requiere que el adversario tenga una cuenta válida ("Authorized Attacker") para iniciar la explotación.
Lateral Movement	**T1210**	*Exploitation of Remote Services*	Si se usa para saltar de un nodo a otro dentro del entorno gestionado.



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

Versiones afectadas.

- **Windows Admin Center (v2):** Todas las versiones anteriores a la **2602** (Build 2.6.2602.0).
- **Windows Admin Center (v1 / Legacy):** Versión **2311** y anteriores (si todavía están en uso en la infraestructura, aunque algunas ya están fuera de soporte, siguen siendo vulnerables).
- **Windows Admin Center Preview:** Builds Insider Preview anteriores a la **2602-preview**.

Indicadores de compromiso

Logs de la Aplicación Windows Admin Center

El canal de eventos principal es Microsoft-ServerManagementExperience.

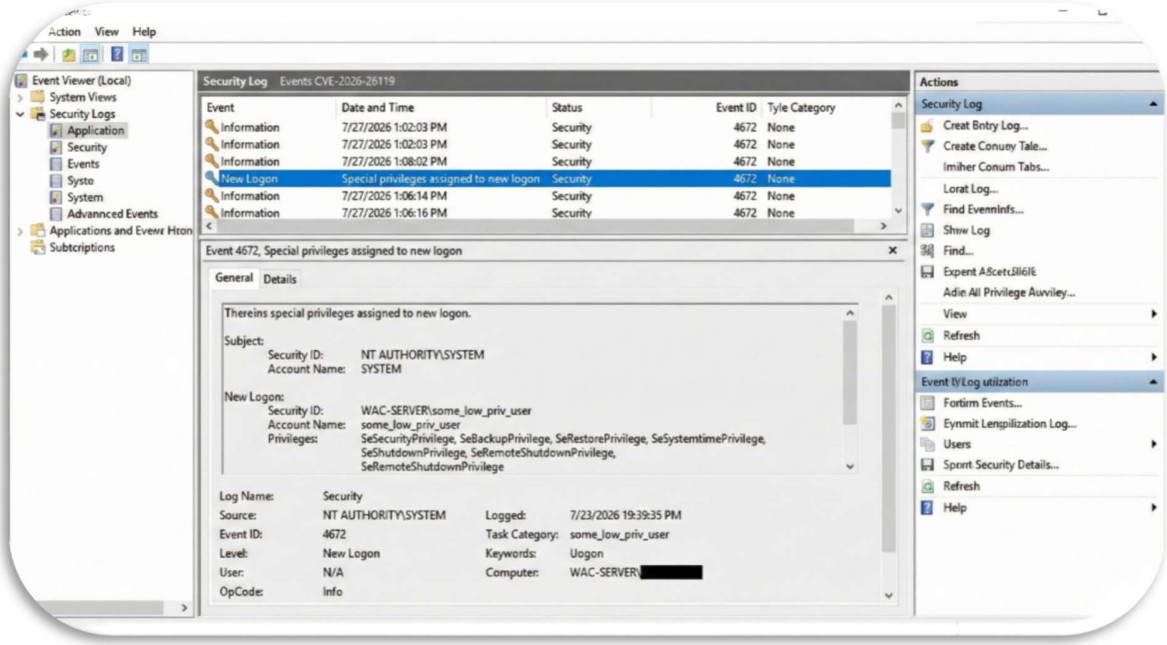
- **Evento Crítico:** Operaciones de escritura (POST/PUT/DELETE) exitosas realizadas por cuentas de bajo privilegio.
- **Ruta del Log:** Applications and Services Logs -> Microsoft -> ServerManagementExperience
- **Patrón de Búsqueda:**
  - Filtrar eventos donde el UserName **NO** pertenezca al grupo "Gateway Administrators" o "Domain Admins".
  - Buscar acciones en la API que modifiquen el estado del sistema, tales como:
    - POST /api/nodes/{server}/features/scripting/invoke (Ejecución de scripts)
    - POST /api/nodes/{server}/features/users/add (Creación de usuarios)
  - **Alerta:** Si ves tráfico a estos endpoints proveniente de una cuenta de servicio (ej. svc_monitor) o un usuario estándar, es un indicador positivo de explotación.

Logs de PowerShell (Script Block Logging)

Dado que WAC utiliza PowerShell por debajo (a través de WinRM), el ataque dejará rastro aquí.

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

- **Event ID 4104 (PowerShell/Operational):**
  - **Contexto:** WAC ejecuta comandos bajo el proceso wsmprovhost.exe.
  - **IoC de Comportamiento:** Buscar bloques de script que contengan comandos de "añadir miembros a grupos" ejecutados remotamente, pero iniciados por una identidad de usuario inusual.
  - **Keywords Sospechosas:**
    - Add-LocalGroupMember
    - net localgroup administrators
    - net group "Domain Admins"
  - **Falso Positivo:** Verificar si el UserContext es el administrador legítimo. Si el UserContext es NT AUTHORITY\NETWORK SERVICE o una cuenta de bajo nivel intentando estos comandos, es un ataque confirmado.



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

Tráfico de Red (Logs de Firewall / WAF)

Si tienes un WAF protegiendo el portal web del Admin Center:

- **Manipulación de Headers:**
  - Solicitudes donde el User-Agent cambia repentinamente dentro de la misma sesión (indicativo de herramientas de explotación automatizada o scripts en Python/Go vs. el navegador legítimo).
- **Volumen de API:**
  - Un usuario que normalmente solo hace "Lectura" (GET dashboard) repentinamente envía una ráfaga de solicitudes POST a /api/.

Recomendaciones

Microsoft ha liberado parches de seguridad en el ciclo de actualizaciones de febrero de 2026.

- **Aplicar el Parche:**

Verificar la versión actual en el icono de "Ayuda" (?) o "Configuración" en la esquina superior derecha de la consola de Windows Admin Center. Si el número de versión es inferior a **2.6.2602.0**, actualice inmediatamente **Windows Admin Center** a la versión más reciente (publicada a partir del 17 de febrero de 2026). Verifique el *Update Guide* de Microsoft para el número de KB específico según su versión (generalmente actualizaciones automáticas si están habilitadas en la extensión).

También se podría hacer de manera controlada la actualización realizando el proceso manualmente y no por Windows Update, se puede realizar de la siguiente manera:

- Obtenga el instalador .msi oficial más reciente (v2602) desde el Centro de Evaluación de Microsoft o el Catálogo de Microsoft Update (https://www.microsoft.com/es-mx/evalcenter/evaluate-windows-admin-center).
- Ejecute el instalador en el servidor donde reside el Gateway.
- El instalador detectará la versión anterior (v2311 o inferior).
- Seleccione la opción **"Actualizar"** (Upgrade).

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

- El instalador preservará la configuración existente (puerto, certificado SSL y lista de conexiones). No es necesario reconfigurar.
- El servicio web se reiniciará (interrupción de aprox. 2-5 minutos en la consola de gestión, **no afecta** a los servidores gestionados).

Mientras se aplica el parche, o como defensa en profundidad:

- **Segmentación de Red:** Asegúrese de que la interfaz de Windows Admin Center no esté expuesta a toda la red interna. Restrinja el acceso solo a las IPs de las estaciones de trabajo de los administradores (Tier 0/1).
- **Principio de Mínimo Privilegio:** Revise qué cuentas tienen acceso, incluso de lectura, al Admin Center. Reduzca la superficie de ataque limitando quién es un "usuario autorizado".
- **Monitoreo Activo:** Configure alertas en su SIEM para detectar el uso de comandos administrativos críticos (ej. PowerShell remoto) iniciados desde la instancia de Windows Admin Center por usuarios inusuales.

Fuentes:

- https://www.microsoft.com/es-mx/evalcenter/evaluate-windows-admin-center
- https://windowsforum.com/threads/cve-2026-26119-privilege-escalation-in-windows-admin-center-on-management-hosts.401576/?amp=1
- https://cybersecuritynews.com/windows-admin-center-escalation-vulnerability/

Este evento presenta un riesgo critico si no se cuentas con las medidas de seguridad bien establecidas iniciando principalmente con actualizaciones de los servidores, la defensa de un servidor ya no se limita a bloquear intrusos externos, sino que requiere una auditoría interna exhaustiva de cada módulo y cada llamada al sistema.

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) 3168931490 - 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