Alerta

Microsoft corrige dos vulnerables explotadas activamente CVE-2026-85880 y CVE-2026-81963

COLCERT AL- 20260912 -118

Resumen Ejecutivo

El 8 de septiembre de 2026, Microsoft publicó correcciones para dos vulnerabilidades de Windows —CVE-2026-85880 y CVE-2026-81963— que posteriormente fueron incorporadas al catálogo de Vulnerabilidades Explotadas Conocidas (KEV) de CISA ante la evidencia de explotación activa.

Ambas requieren acceso local previo, no exigen interacción del usuario y permiten escalar privilegios hasta SYSTEM, convirtiendo un acceso inicial limitado en el control total del equipo.

IMPACTO	EXPLOTACIÓN	SISTEMAS PRIORITARIOS	ACCIÓN INMEDIATA
Elevación de privilegios hasta SYSTEM	Explotación activa confirmada e inclusión en CISA KEV	Servidores Windows, estaciones administrativas, RDS, jump servers y equipos SOC/TI	Aplicar las actualizaciones acumulativas de septiembre de 2026 y validar KB, compilación y reinicio

PLAZO DE REMEDIACIÓN KEV: 22 DE SEPTIEMBRE DE 2026

¿Qué permiten hacer estas vulnerabilidades?

- ❑ Escalar privilegios locales hasta SYSTEM, sin interacción del usuario.
- ❑ Escapar del aislamiento de un AppContainer o abusar del Windows Update Stack para elevar privilegios.
- ❑ Convertir un acceso inicial limitado en control total del equipo.

¿Por qué esta alerta es prioritaria?

- ❑ Explotación activa confirmada e incorporación al catálogo KEV de CISA.
- ❑ Afectan a casi todas las ediciones soportadas de Windows. tanto cliente como Server.
- ❑ El acceso a SYSTEM facilita la persistencia, la evasión de controles y el movimiento lateral posterior.

NIVEL DE RIESGO

ALTO

CVE	Componente, vector e impacto	CVSS 3.1 / CWE
CVE-2026-85880	Windows Advanced Local Procedure Call — desbordamiento de búfer. Código de bajo privilegio dentro de un AppContainer puede escapar del aislamiento y elevar a SYSTEM; sin interacción.	7,8 Alta — AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H; CWE-122 y CWE-908
CVE-2026-81963	Windows Update Stack — resolución incorrecta de enlaces antes de acceder a archivos. Un usuario o código local de bajo privilegio puede manipular enlaces y elevar a SYSTEM; sin interacción.	7,8 Alta — AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H; CWE-59

Detalles técnico de las vulnerabilidades

Ambas vulnerabilidades requieren acceso local previo (AC:L, PR:L) pero no exigen interacción del usuario (UI:N): un acceso inicial limitado basta para escalar a SYSTEM.

Vector técnico de cada vulnerabilidad

- CVE-2026-85880: desbordamiento de búfer en Windows ALPC; permite escapar del aislamiento de un AppContainer.
- CVE-2026-81963: resolución incorrecta de enlaces en el stack de Windows Update.
- Ambas escalan desde privilegio bajo a SYSTEM sin interacción del usuario.
- Explotación registrada por Microsoft; aún no se han detallado cadenas de ataque completas.

Microsoft y CISA no han publicado firmas ni artefactos forenses específicos para estas dos CVE; la evidencia de explotación proviene de su inclusión oficial en el catálogo KEV.

Señales de alerta ¿qué comportamientos debo monitorear?

A la fecha, Microsoft y CISA no han publicado IoC o artefactos forenses específicos asociados a la explotación de estas vulnerabilidades. No obstante, como medida de monitoreo, se recomienda prestar atención a comportamientos anómalos compatibles con las técnicas de escalada descritas:

- Ejecuciones originadas desde un AppContainer que deriven en procesos, servicios o tokens con privilegios SYSTEM.
- Creación anómala de enlaces simbólicos, junctions o puntos de análisis asociados a directorios utilizados por Windows Update.
- Escrituras realizadas por procesos privilegiados inmediatamente después de actividad de actualización.
- Creación inusual de procesos hijos, tareas programadas, cuentas locales o exclusiones de Microsoft Defender tras eventos o fallos relacionados con ALPC.

Cronología y estado de explotación

Hito	Fecha	Detalle
Publicación de parches	8-sep-2026	Microsoft libera actualizaciones para ambas CVE
Inclusión en catálogo KEV	8-sep-2026	CISA, por explotación activa confirmada
Plazo de remediación KEV	22-sep-2026	Fecha límite fijada por CISA
PoC / detalles de campaña	No publicados	Microsoft no ha revelado la cadena de ataque
IoC específicos	No publicados	Sin artefactos forenses oficiales disponibles
Puntuación EPSS	Pendiente	FIRST aún no publica puntuación ni percentil

Discrepancia relevante: el CVSS base de 7,8 corresponde a una vulnerabilidad local; la explotación confirmada por Microsoft y la inclusión en KEV elevan materialmente la prioridad frente a una evaluación basada solo en la puntuación.

Inferencia: ambas vulnerabilidades pueden emplearse como segunda fase tras un evento de phishing, explotación web o uso de credenciales comprometidas; Microsoft no ha atribuido públicamente una cadena de ataque concreta.

Recomendaciones para detección y monitoreo

Las organizaciones deben prestar especial atención a comportamientos que puedan sugerir un intento de escalada de privilegios, entre los cuales se destacan:

- ❑ Configurar alertas para procesos originados en un AppContainer que deriven en tokens SYSTEM.
- ❑ Correlacionar eventos de Windows Update con la creación de enlaces simbólicos o junctions.
- ❑ Monitorear cuentas locales, tareas programadas o exclusiones de Defender creadas tras fallos ALPC.
- ❑ Mantener actualizadas las firmas y reglas de EDR para ambas técnicas de escalada.

La correlación temprana de estos eventos puede permitir detectar un intento de escalada de privilegios antes de que se traduzca en control total del equipo.

Recomendaciones de prevención

Regla Prioritaria: despliegue de inmediato las actualizaciones acumulativas de septiembre de 2026, priorizando controladores de dominio, servidores de salto (jump servers) y estaciones SOC/TI. Posteriormente, reinicie los sistemas cuando corresponda y verifique el KB instalado y el número de compilación, antes de considerar finalizado el proceso de remediación.

Medidas de mitigación inmediata

- ❑ Desplegar de inmediato las actualizaciones acumulativas de septiembre de 2026, priorizando activos privilegiados y servidores.
- ❑ Aislar o restringir los equipos que no puedan actualizarse de forma inmediata.
- ❑ Retirar privilegios locales innecesarios y reforzar controles WDAC/AppLocker.
- ❑ Reforzar la protección contra alteraciones y los controles EDR sobre procesos de bajo privilegio.

Validación de versiones y parches

La versión segura depende del sistema y de la actualización de septiembre de 2026; antes de cerrar el parcheo, se recomienda:

- ❑ Confirmar el KB y número de compilación efectivo aplicado en cada equipo, según las tablas de Microsoft.
- ❑ Verificar que el reinicio posterior a la actualización se completó correctamente.
- ❑ Revisar la cobertura en Windows cliente y Windows Server, sin asumir que todas las ediciones comparten el mismo KB.
- ❑ Registrar la evidencia de aplicación del parche como parte del cierre del hallazgo.

Cuando la actualización requiera reinicio, la remediación no debe considerarse finalizada hasta completar el reinicio y verificar el KB y la compilación instalada.

¿Qué hacer ante indicios de explotación?

- ❑ Aislar el equipo afectado de la red inmediatamente.
- ❑ Preservar memoria RAM y los registros del sistema antes de cualquier reinicio.
- ❑ Investigar procesos hijos, servicios o tareas programadas creados inmediatamente después de fallos ALPC o actividad de Windows Update.
- ❑ Rotar las credenciales privilegiada que hayan sido utilizadas en el equipo.
- ❑ Documentar la hora del evento, hallazgos y acciones realizadas.
- ❑ Notificar el incidente al área interna de seguridad de la información y, tras su clasificación, escalarlo al CSIRT Gobierno / ColCERT.

¿Sabe si su organización está expuesta?

El ColCERT incluye, dentro de su portafolio de servicios, la ejecución de análisis especializados de vulnerabilidades en sitios web, servidores y demás activos de información. Estos escaneos permiten identificar de manera proactiva brechas de seguridad, configuraciones deficientes y exposiciones críticas, entregando los insumos técnicos necesarios para que las organizaciones puedan aplicar medidas de mitigación y fortalecer su postura de ciberseguridad.

Adicionalmente, el ColCERT, tiene la capacidad de efectuar revisiones específicas sobre entornos institucionales de Active Directory (Directorio Activo) para evaluar su nivel de hardening (endurecimiento) y la configuración básica de seguridad.

Para más información, le invitamos a comuníquese a través de los canales oficiales del CSIRT Gobierno / ColCERT.

Conéctate con el ColCERT:

contacto@colcert.gov.co

Línea directa:
+57 601 344 2222

Fuentes

❑ Microsoft — avisos de seguridad CVE-2026-85880 y CVE-2026-81963.

❑ Microsoft — notas de la actualización acumulativa de septiembre de 2026.

❑ Microsoft — notas de la actualización acumulativa de septiembre de 2026.

❑ CISA — catálogo de Vulnerabilidades Explotadas Conocidas (KEV).

❑ CVE.org — registros CVE-2026-85880 y CVE-2026-81963.

❑ NVD — entradas para ambas CVE.

❑ FIRST — EPSS (puntuación pendiente de publicación).