Microsoft publicó sus actualizaciones mensuales de seguridad el martes, y una de las vulnerabilidades corregidas ya está siendo aprovechada activamente en ataques.

El fallo se encuentra en un controlador central del kernel de Windows encargado de gestionar operaciones de sockets de red. Un atacante que ya haya logrado ejecutar código en un equipo puede explotar esta vulnerabilidad para elevar privilegios hasta SYSTEM. Por ello, esta actualización debe considerarse la máxima prioridad.

La vulnerabilidad está identificada como CVE-2026-68820 (puntuación CVSS: 7.0) y es la única de este mes que Microsoft señala como explotada activamente. Su explotación requiere desencadenar una condición de carrera dentro del controlador afectado. Microsoft no ha atribuido públicamente los ataques observados. Sin embargo, *Check Point Research* afirma que el grupo Lazarus utilizó este día cero durante su campaña *Operation Dream Job*.

Otras cuatro vulnerabilidades incluidas en la actualización no requieren ninguna interacción por parte de la víctima: no necesitan credenciales, autenticación ni acciones del usuario. Estas afectan a Windows DNS Server, Windows Deployment Services, la implementación de Microsoft del protocolo de transporte QUIC y High Performance Computing (HPC) Pack. Cada una posee una puntuación CVSS de 9.8. Ninguna estaba marcada como explotada cuando se publicaron los parches.

Según un recuento independiente, la *Zero Day Initiative* contabilizó 398 nuevos CVE, de los cuales 62 fueron clasificados como Críticos. Estas cifras reflejan la magnitud de la actualización, aunque el orden de aplicación de los parches debe basarse principalmente en el estado de explotación y en el alcance potencial de cada vulnerabilidad.

La actualización también corrige la parte de ejecución remota de código (RCE) de una cadena de ataque de SharePoint cuya vulnerabilidad de omisión de autenticación fue solucionada en julio. Las implementaciones locales de SharePoint deberían tener instaladas ambas actualizaciones.

Check Point Research indicó que CVE-2026-68820 corresponde a una vulnerabilidad de tipo

use-after-free en afd.sys, el *Ancillary Function Driver for WinSock* y componente del subsistema de red de Windows que opera a nivel de kernel.

Se trata de una vulnerabilidad de escalación de privilegios: el atacante debe contar previamente con ejecución de código en el sistema y posteriormente puede utilizar el fallo para obtener privilegios SYSTEM. Microsoft la clasifica como explotada activamente, lo que la sitúa por encima de las cuatro vulnerabilidades de ejecución remota con puntuación 9.8, a pesar de tener una calificación CVSS menor.

Sin necesidad de interacción de la víctima

Las cuatro vulnerabilidades de ejecución remota de código sin autenticación deben atenderse inmediatamente después del fallo del controlador explotado activamente, ya que permiten ejecutar código en servidores sin requerir una cuenta válida ni intervención de usuarios.

1. CVE-2026-62878, Windows DNS Server.
   Vulnerabilidad de desbordamiento de búfer basado en pila accesible de forma remota, sin autenticación ni interacción del usuario. La *Zero Day Initiative* describe esta condición como «wormable» (capaz de propagarse como un gusano), aunque Microsoft considera menos probable su explotación. El término utilizado por ZDI se refiere únicamente a las características técnicas de la vulnerabilidad y no implica que exista actualmente un gusano explotándola.
2. CVE-2026-62893, Windows Deployment Services.
   Vulnerabilidad remota accesible a través del manejo del protocolo TFTP del servicio, sin requerir autenticación ni acciones del usuario.
3. CVE-2026-62815, Microsoft QUIC.
   Vulnerabilidad de ejecución remota de código accesible de manera remota, sin autenticación y sin interacción de la víctima.
4. CVE-2026-59124, HPC Pack.
   Aunque comparte la puntuación CVSS de 9.8, Microsoft la clasifica como Importante en lugar de Crítica, debido a que HPC Pack no se instala de forma predeterminada.

> Microsoft considera que la probabilidad de explotación es mayor.

Dado que HPC Pack no viene instalado por defecto, la prioridad práctica de esta y de las otras vulnerabilidades dependerá de si los servicios vulnerables están presentes y accesibles dentro de cada entorno. Por ello, al definir prioridades de remediación, deben considerarse tanto el inventario de servicios y su exposición como el estado de explotación conocido.

Se completa una cadena de ataque de SharePoint

La actualización de agosto también finaliza una corrección de SharePoint iniciada durante julio.

Rapid7 Labs informó a Microsoft el 18 de mayo sobre una cadena de explotación que combinaba una vulnerabilidad de omisión de autenticación con otra de ejecución remota de código para *obtener ejecución remota de código sin autenticación en implementaciones locales de SharePoint*. Dos días después, Microsoft confirmó que dividiría la mitigación entre los ciclos de actualización de julio y agosto.

En julio se corrigió la primera parte de la cadena mediante CVE-2026-55040, una vulnerabilidad crítica de omisión de autenticación con una puntuación de 9.1. Según *Rapid7*, este fallo permitía que un atacante remoto no autenticado asumiera la identidad de un usuario o administrador de SharePoint, siempre que conociera previamente la identidad que deseaba suplantar. La actualización de agosto incorpora la corrección para el componente de ejecución remota de código, identificado como CVE-2026-63520.

La diferencia es relevante: CVE-2026-63520 corresponde exclusivamente al componente de ejecución de código de la cadena de ataque y, por sí sola, no proporciona acceso sin autenticación. La capacidad de lograr ejecución remota sin autenticación surgía al combinar esta vulnerabilidad con CVE-2026-55040.

Rapid7 señala que la aplicación del parche de CVE-2026-55040 ya interrumpía la cadena de explotación demostrada, por lo que esa vía quedó cerrada desde la actualización de julio.

Con la actualización de agosto se elimina además el componente de ejecución remota de código.

Recomendaciones de prioridad

- Priorizar CVE-2026-68820 en sistemas Windows donde un atacante pueda disponer ya de ejecución de código y utilizar el fallo para obtener privilegios SYSTEM.
- A continuación, aplicar los parches para los servicios expuestos de DNS, WDS, QUIC y HPC Pack.
- Verificar que todas las implementaciones locales de SharePoint cuenten tanto con el parche de julio para la omisión de autenticación (CVE-2026-55040) como con la corrección de agosto para la ejecución remota de código (CVE-2026-63520).