Microsoft ha revelado que una vulnerabilidad de escalada de privilegios y otra de denegación de servicio en Defender están siendo explotadas activamente en entornos reales.

La primera, identificada como CVE-2026-41091, posee una calificación de 7.8 en el sistema CVSS. Si es explotada con éxito, podría permitir que un atacante obtenga privilegios de nivel SYSTEM.

"Una resolución incorrecta de enlaces antes del acceso a archivos ('link following') en Microsoft Defender permite que un atacante autorizado eleve privilegios localmente", señaló Microsoft en un comunicado.

La segunda vulnerabilidad explotada es CVE-2026-45498 (CVSS: 4.0), un fallo de denegación de servicio que afecta a Defender. Ambas vulnerabilidades fueron corregidas en las versiones 1.1.26040.8 y 4.18.26040.7 de Microsoft Defender Antimalware Platform, respectivamente.

La compañía tecnológica indicó que los sistemas que tienen Microsoft Defender deshabilitado no son vulnerables a este problema. Además, aclaró que no es necesario realizar acciones manuales para instalar la actualización, ya que las definiciones de malware y el motor Microsoft Malware Protection Engine se actualizan automáticamente para garantizar una protección óptima.

Microsoft atribuyó el hallazgo y reporte de estas fallas a cinco investigadores distintos: Sibusiso, Diffract, Andrew C. Dorman (también conocido como ACD421), Damir Moldovanov y un investigador anónimo.

Para verificar que la versión más reciente de Microsoft Malware Protection Platform y las actualizaciones de definiciones se estén descargando e instalando correctamente, se recomienda seguir estos pasos:

- Abrir la aplicación Seguridad de Windows.
- En el panel de navegación, seleccionar Protección contra virus y amenazas.
- Hacer clic en Actualizaciones de protección dentro de la sección correspondiente.

- Seleccionar Buscar actualizaciones.
- En el panel lateral, acceder a Configuración y luego a Acerca de.
- Revisar el número de versión del cliente antimalware.

Hasta el momento, no se han revelado detalles sobre la forma en que estas vulnerabilidades están siendo explotadas en ataques reales. La Agencia de Ciberseguridad y Seguridad de Infraestructura de Estados Unidos (CISA) añadió ambas fallas a su catálogo Known Exploited Vulnerabilities (KEV), exigiendo a las agencias del Federal Civilian Executive Branch (FCEB) aplicar los parches antes del 3 de junio de 2026.

Con este nuevo incidente, ya son tres las vulnerabilidades de Microsoft marcadas como explotadas activamente en menos de una semana. La semana pasada, la empresa de Redmond informó que una falla de cross-site scripting en versiones locales de Exchange Server (CVE-2026-42897, CVSS: 8.1) había sido utilizada en ataques reales.

Asimismo, el miércoles se incorporaron al catálogo KEV otras cuatro vulnerabilidades antiguas de Microsoft correspondientes a 2008, 2009 y 2010:

- CVE-2010-0806 – Microsoft Internet Explorer presenta una vulnerabilidad *use-after-free* que podría permitir a atacantes remotos ejecutar código arbitrario.
- CVE-2010-0249 – Microsoft Internet Explorer contiene otra vulnerabilidad *use-after-free* capaz de facilitar la ejecución remota de código arbitrario.
- CVE-2009-1537 – Microsoft DirectX incluye una vulnerabilidad de sobrescritura de byte NULL en el filtro QuickTime Movie Parser de quartz.dll en DirectShow, lo que podría permitir la ejecución remota de código mediante un archivo multimedia QuickTime manipulado.
- CVE-2008-4250 – Microsoft Windows presenta una vulnerabilidad de desbordamiento de búfer en el servicio Windows Server Service que posibilita la ejecución remota de código a través de una solicitud RPC especialmente diseñada.

Otra vulnerabilidad mencionada en la lista es CVE-2009-3459, un desbordamiento de búfer basado en heap presente en Adobe Acrobat y Reader, que podría permitir a atacantes

remotos ejecutar código arbitrario mediante un archivo PDF manipulado que provoque corrupción de memoria.