Boletín de alerta

Boletín Nro.:
Fecha de publicación: 14/07/2026
Tema: Alerta 2026-69 Microsoft Tuesday Patch
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Microsoft Windows 10 y Windows 11
- Windows Server
- Microsoft SharePoint Server
- Active Directory Federation Services (AD FS)
- Microsoft Office
- Microsoft .NET y ASP.NET Core
- Microsoft Azure
- Windows SMB Server
- Windows Kernel
- Windows Admin Center
- Microsoft SQL Server
- Microsoft Edge (Chromium)

Descripción

Microsoft publicó las actualizaciones de seguridad correspondientes al **Patch Tuesday de julio de 2026**, corrigiendo **570 vulnerabilidades** en sus productos. Entre ellas se incluyen **tres vulnerabilidades Zero-Day**, varias fallas críticas de ejecución remota de código (RCE) y múltiples vulnerabilidades de elevación de privilegios (EoP). Este lanzamiento representa uno de los ciclos de actualización más importantes del año debido al volumen de vulnerabilidades y a la presencia de fallas que ya estaban siendo explotadas antes de la publicación de los parches.

A continuación se describen las cinco vulnerabilidades más relevantes.

CVE-2026-56155 – Active Directory Federation Services Elevation of Privilege (CVSS 8.8): Esta vulnerabilidad afecta Active Directory Federation Services (AD FS) y permite a un atacante elevar privilegios dentro del entorno de autenticación federada. Un atacante con acceso previo podría obtener permisos superiores y comprometer los servicios de identidad utilizados por aplicaciones locales y en la nube. Microsoft confirmó que esta vulnerabilidad estaba siendo explotada activamente antes de la

publicación del parche.

CVE-2026-56164 – Microsoft SharePoint Server Remote Code Execution (CVSS 9.8): Esta vulnerabilidad crítica afecta Microsoft SharePoint Server y permite la ejecución remota de código mediante solicitudes especialmente diseñadas dirigidas al servidor. La explotación exitosa podría permitir que un atacante tome control completo del servidor SharePoint, acceda a documentos corporativos y utilice el servidor como punto de apoyo para comprometer el resto de la infraestructura.

CVE-2026-50661 – Windows Remote Code Execution Vulnerability (CVSS 9.8): Esta vulnerabilidad permite que un atacante remoto ejecute código arbitrario enviando tráfico especialmente diseñado al sistema vulnerable. La explotación no requiere interacción significativa del usuario y puede conducir al compromiso completo del equipo afectado.

CVE-2026-50522 – Microsoft SharePoint Server (CVSS 9.8): La vulnerabilidad crítica afecta a Microsoft SharePoint Server local y permite la ejecución remota de código sin autenticación (CVSS 9.8). La falla, causada por una deserialización de datos no confiables, está siendo explotada activamente para robar las claves de máquina de SharePoint y mantener acceso persistente. Aplicar únicamente los parches no es suficiente; también es necesario rotar las claves de máquina y las credenciales potencialmente comprometidas para evitar que los atacantes conserven el acceso al entorno

CVE-2026-54121 – Active Directory Certificate Services (AD CS) (CVSS 8.8)

Es una vulnerabilidad de elevación de privilegios en AD CS. La falla se debe a una autorización incorrecta que permite a un usuario autenticado con privilegios limitados obtener privilegios elevados dentro del dominio. Actualmente, ya existe una prueba de concepto (PoC) pública que demuestra su explotación, la cual permite solicitar un certificado de un controlador de dominio, autenticarse como dicho controlador y ejecutar un ataque DCSync para extraer el secreto KRBTGT, lo que puede derivar en el compromiso total del dominio de Active Directory.

CVE-2026-57089 – Windows SMB Server Network Transport Driver Remote Code Execution (CVSS 7.5): La vulnerabilidad afecta al controlador srvnet.sys utilizado por SMB Server, permitiendo ejecución remota de código mediante paquetes de red especialmente construidos. Aunque requiere ciertas condiciones de explotación, representa un riesgo considerable para servidores Windows expuestos dentro de redes corporativas.

CVE-2026-58631 – Windows Admin Center Remote Code Execution (CVSS 8.8): Esta vulnerabilidad afecta Windows Admin Center, la consola de administración remota utilizada para administrar servidores Windows. Un atacante autenticado podría ejecutar código arbitrario en el servidor que aloja Windows Admin Center.

Empresas de inteligencia de amenazas han observado intentos activos de explotación de las tres vulnerabilidades en entornos reales. Aunque inicialmente Fortinet indicó que las fallas no estaban siendo explotadas, investigadores independientes detectaron actividad maliciosa dirigida contra dispositivos vulnerables pocos días después de la publicación de los parches.

Solución

Microsoft recomienda implementar las actualizaciones de seguridad lo antes posible y priorizar especialmente los sistemas expuestos a Internet.

- Instalar inmediatamente las actualizaciones del **Patch Tuesday de julio de 2026**.
- Priorizar servidores SharePoint, AD FS y Windows Admin Center.
- Actualizar todos los controladores de dominio y servidores Windows.
- Verificar que Windows Update, WSUS o Microsoft Configuration Manager hayan distribuido correctamente los parches.
- Revisar los boletines de Microsoft para conocer requisitos específicos de reinicio y posibles mitigaciones temporales.

Información adicional:

- Microsoft Security Update Guide
- BleepingComputer – Microsoft July 2026 Patch Tuesday
- Zero Day Initiative – July 2026 Security Update Review
- Help Net Security – July 2026 Patch Tuesday Forecast