# Boletín de alerta

**Boletín Nro.:** 37
**Fecha de publicación:** 15/04/2026
**Tema:** Alerta 2026-37 Patch Tuesday abril 2026: vulnerabilidad de spoofing en SharePoint (CVE-2026-32201) y 0 day en Microsoft Defender
**Traffic Light Protocol (TLP):** White

## Actualizado: 15/04/2026

## Producto(s) afectado(s):

- SharePoint Server 2016
- SharePoint Server 2019
- SharePoint Server Subscription Edition

Otros productos de Microsoft (Windows, Office, Microsoft Defender, etc.) también reciben actualizaciones de seguridad en este boletín, pero se listan aquí únicamente las plataformas afectadas por CVE 2026 32201.

## Descripción

Se ha publicado el boletín de abril de 2026 de **Microsoft** (Patch Tuesday), que corrige un total de 163 vulnerabilidades clasificadas entre críticas e importantes en múltiples productos, incluyendo **Windows, Office, Microsoft Defender** y, de forma destacada, **Microsoft SharePoint Server**. Entre ellas sobresalen **CVE-2026-32201**, una vulnerabilidad de *spoofing* en SharePoint que ya estaba siendo explotada activamente como día cero antes de la liberación de los parches, y **CVE-2026-33825**, un 0 day en Microsoft Defender que permite a un atacante con acceso local elevar privilegios hasta SYSTEM mediante el abuso del proceso de actualización de la plataforma antimalware.

**CVE-2026-32201** es una vulnerabilidad de **validación de entrada insuficiente** en Microsoft Office SharePoint que permite a un atacante remoto no autenticado realizar ataques de *spoofing* sobre la aplicación a través de la red. Mediante peticiones especialmente manipuladas, el atacante puede lograr que SharePoint acepte o genere contenido en nombre de otro usuario o contexto, con capacidad para **ver información sensible y modificar datos que queden "suplantados" en la respuesta**. Microsoft y distintos analistas la clasifican como **Importante**, con **CVSS v3.1 6.5**, pero con señal clara de **explotación activa en servidores SharePoint expuestos a Internet**.

Además de CVE-2026-32201, el paquete de abril incluye otras vulnerabilidades de severidad crítica en componentes de Windows (elevación de privilegios, RCE) y otra vulnerabilidad de *spoofing* en SharePoint,

**CVE-2026-20945**, con CVSS 4.6 pero que se corrige en las mismas actualizaciones. En conjunto, el boletín destaca un volumen elevado de fallos de elevación de privilegios (más del 50% del total), así como un número significativo de vulnerabilidades de divulgación de información y RCE que afectan a sistemas de escritorio y servidores.

En entornos donde **SharePoint está expuesto a Internet o accesible desde redes menos confiables**, esta vulnerabilidad puede permitir a un atacante remoto sin credenciales **suplantar identidades o contexto de usuario**, accediendo a información que no debería ver o modificando contenido dentro de sitios SharePoint.

Dado que SharePoint suele integrarse con repositorios documentales internos, intranets y flujos de trabajo corporativos, la explotación puede derivar en **pérdida de confidencialidad, manipulación de documentos y riesgo de movimiento lateral**, especialmente si se combina con otras vulnerabilidades de elevación de privilegios.

Ademas, Microsoft incluyó en el Patch Tuesday de abril una corrección para un **0□day en Microsoft Defender**, rastreado como **CVE-2026-33825**, clasificado como vulnerabilidad de **elevación de privilegios** con **CVSS 7.8 (Importante)**. El fallo, relacionado con el manejo del proceso de actualización de la plataforma antimalware, permite que un atacante con acceso local abuse de Defender para **elevar sus privilegios hasta SYSTEM**, convirtiendo un compromiso limitado (por ejemplo, una cuenta estándar) en control total del sistema.

A diferencia de otras vulnerabilidades de ejecución remota, este 0□day requiere que el atacante ya tenga algún tipo de presencia en el equipo, pero se considera especialmente sensible porque **afecta directamente al componente de seguridad integrado en Windows**, y porque el exploit ("BlueHammer") fue publicado públicamente antes de disponerse de parche, aumentando el riesgo de reutilización por parte de actores maliciosos. Microsoft ha mitigado el problema mediante una actualización de la **Microsoft Defender Antimalware Platform** (versión 4.18.26050.3011 o superior), que se distribuye de forma automática a través del canal habitual de actualizaciones de Defender, por lo que se recomienda verificar que todos los endpoints han recibido ya esta versión y, en entornos críticos, forzar la actualización manualmente.

## Solución:

Microsoft ha publicado actualizaciones acumulativas de seguridad para **SharePoint Server 2016, 2019 y SharePoint Server Subscription Edition**, que corrigen tanto CVE-2026-32201 como CVE-2026-20945. Se recomienda:

- **Aplicar de forma prioritaria las actualizaciones de abril 2026** en todos los servidores SharePoint, empezando por aquellos expuestos a Internet o accesibles desde redes DMZ.
- Verificar tras el parcheo que las versiones instaladas corresponden a los KB indicados en la documentación de Microsoft para cada producto.
- Revisar logs de acceso de SharePoint en busca de actividad anómala asociada a peticiones manipuladas o patrones de *spoofing*, dado que CVE-2026-32201 ha sido reportada como **explotada**

**en la práctica**.

| Producto | Estado sin parche | Actualización que corrige CVE-2026-32201 |
|---|---|---|
| *SharePoint Server 2016* | *Vulnerable* | *KB5002861 (actualización de seguridad 14/04/2026)* |
| *SharePoint Server 2019* | *Vulnerable* | *Actualización de seguridad de abril 2026 (KB según edición)* |
| *SharePoint Server Subscription Edition* | *Vulnerable* | *Actualización de seguridad de abril 2026 (Subscription Edition, KB específico)* |

A continuación se listan las guías proveidas por el fabricante:

- **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201**
- **https://support.microsoft.com/help/5002861**

Además, se recomienda verificar que todos los equipos Windows tengan actualizada la plataforma de Microsoft Defender a la versión 4.18.26050.3011 o superior, ya que el mismo boletín corrige la vulnerabilidad de elevación de privilegios CVE 2026 33825 explotada como 0 day.

## Información adicional:

- **https://nvd.nist.gov/vuln/detail/CVE-2026-32201**
- **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201**
- https://www.tenable.com/blog/microsofts-april-2026-patch-tuesday-addresses-163-cves-cve-2026-32201