

Boletín de alerta

Boletín Nro.: 102

Fecha de publicación: 17/09/2026

Tema: Alerta 2026-102 Vulnerabilidades críticas en The Events Calendar plugin para WordPress

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	CVE	Versiones afectadas	Versión corregida
The Events Calendar para WordPress	CVE-2026-78159	Hasta la 6.17.3, inclusive	6.17.3.1 o posterior
The Events Calendar para WordPress	CVE-2026-78006	Hasta la 6.17.4, inclusive	6.17.4.1 o posterior
The Events Calendar para WordPress	Ambas vulnerabilidades	Versiones previas a la 6.17.4.1	6.17.4.1 o posterior

*La versión **6.17.4.1**, publicada el 10 de septiembre de 2026, es la primera release que contiene correcciones para las dos vulnerabilidades.

Descripción

Se identificaron dos vulnerabilidades críticas de ejecución remota de código (RCE) en el plugin **The Events Calendar** para WordPress, desarrollado por StellarWP. Las fallas, **CVE 2026 78006** y **CVE 2026 78159**, tienen puntuación **CVSS 9.8** y permiten a atacantes remotos no autenticados tomar control de sitios vulnerables bajo determinadas condiciones, sin requerir registro, inicio de sesión ni interacción de una víctima.

El plugin cuenta con más de **600.000 instalaciones activas**. StellarWP publicó correcciones para ambas cadenas de vulnerabilidades; se recomienda actualizar inmediatamente a **The Events Calendar 6.17.4.1 o una versión posterior** y realizar una revisión de posible compromiso, en particular si el sitio permite comentarios en las páginas individuales de eventos.

Las vulnerabilidades se localizan en el proceso de renderizado de widgets de The Events Calendar, particularmente cuando el plugin procesa contenido de una página individual de evento, incluidos comentarios pendientes de moderación. El atacante no necesita que el comentario sea aprobado: WordPress permite a quien publicó un comentario consultar su propio comentario pendiente mediante un

enlace de moderación, lo que puede hacer que el contenido controlado por el atacante llegue a la lógica vulnerable del plugin.

CVE	CVSS	Tipo	Condición principal	Impacto
CVE 2026 78006	9.8 — Crítica	PHP Object Injection	Comentarios habilitados en páginas de eventos y opción “Show comments on event pages” activa	Ejecución de comandos del sistema y RCE con permisos del usuario del servidor web
CVE 2026 78159	9.8 — Crítica	Inyección de código mediante <i>callable</i> <i>invocation</i> / validación insuficiente	Procesamiento de contenido controlado dentro de widgets de eventos	Restablecimiento de contraseñas administrativas, acceso administrador y posterior RCE

Solución

La solución definitiva es actualizar **The Events Calendar** a la versión **6.17.4.1 o posterior**:

The Events Calendar

Dado que es un RCE critico, de facil explotación, se recomienda luego de actualizarlo seguir los siguiente pasos de verificación:

1. Purgar cachés de WordPress, PHP, CDN y WAF para garantizar que se cargue el código actualizado.
2. Confirmar que no haya comentarios habilitados en páginas de eventos si esa funcionalidad no es requerida.
3. Revisar cuentas administrativas, plugins, archivos y logs para descartar explotación previa.
4. Si se identifican indicios de compromiso, aislar el sitio, preservar evidencia, restaurar desde una copia confiable y rotar credenciales de WordPress, hosting, base de datos, SFTP/SSH, APIs y servicios integrados.

Información adicional:

- [Wordfence — Wordfence Argus Identifies Two Critical Unauthenticated Vulnerability Chains Leading to Remote Code Execution in The Events Calendar Plugin](#)
- [Wordfence Intelligence — CVE?2026?78159](#)
- [SecurityWeek — Unauthenticated RCE Flaws Could Expose 200,000+ WordPress Sites to Takeover](#)
- [Cyber Security News — Critical WordPress Plugin Flaws Put Over 600,000 Websites at Risk of Takeover](#)