Boletín de alerta

Boletín Nro.: 84
Fecha de publicación: 05/08/2026
Tema: Alerta 2026-84 Escritura de Archivos y RCE vía GeoDjango (CVE-2026-15307)
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Django — Framework web de alto nivel para Python

Versión	Estado
Django main (rama de desarrollo)	Vulnerable
Django 6.1 (release candidate)	Vulnerable
Django 6.0 (hasta 6.0.7)	Vulnerable
Django 5.2 (hasta 5.2.16)	Vulnerable

Las ramas anteriores no soportadas (5.0.x, 4.2.x, 4.1.x, 3.2.x) **no fueron evaluadas** y podrían estar igualmente afectadas.

Descripción

Recientemente fue divulgada una vulnerabilidad de severidad alta en el componente **GeoDjango** del framework Django que permite a un atacante autenticado con permisos de visualización sobre modelos con campos espaciales provocar **escritura arbitraria de archivos en el servidor** y, dependiendo del driver de raster activo, ejecutar **código remoto (RCE)**. La falla también habilita ataques de tipo **SSRF** (Server-Side Request Forgery), permitiendo acceder a sistemas internos o metadatos de entornos cloud.

Campo	Detalle
CVE	CVE-2026-15307
Severidad	Alta (High)
CWE	CWE-918 (SSRF) / escritura de archivos del lado del servidor
Componente	GeoDjango — spatial lookups (filtrado en vistas de administración)
Autenticación requerida	Sí — usuario staff con permiso de vista sobre modelos con campos espaciales

El problema reside en que los **spatial lookups** de GeoDjango analizan de forma optimista el valor del lado derecho de una consulta sin validar ni sanitizar adecuadamente la entrada. Un atacante que controle ese valor puede:

1. **Escritura de archivos:** Aprovechar el driver de raster activo para escribir archivos arbitrarios en el sistema de archivos del servidor, lo que en ciertos escenarios puede derivar en **ejecución remota de código**.
2. **SSRF:** Forzar al servidor a realizar solicitudes HTTP hacia sistemas internos o endpoints de metadatos de cloud (AWS IMDSv1, GCP metadata, etc.), exponiendo credenciales o configuraciones sensibles.

El vector de explotación más probable es el **panel de administración de Django** mediante el filtrado en changelists de modelos que contengan campos espaciales (RasterField, GeometryField, etc.).

El parche introduce un cambio **incompatible hacia atrás** — Django ahora bloquea valores de tipo dict y cadenas no seguras en spatial lookups. Algunas consultas existentes podrían verse afectadas y requerir ajustes en el código.

Mitigación

Mientras se aplica el parche:

- **Restringir el acceso al panel de administración** a IPs de confianza o a través de VPN.
- **Revisar qué modelos exponen campos espaciales** en el admin y, si es posible, deshabilitar temporalmente el filtrado en esos changelists.
- **Auditar permisos de usuarios staff**: eliminar permisos de vista sobre modelos con campos espaciales a usuarios que no los requieran estrictamente.
- **Revisar la guía de seguridad de raster** de Django antes de aplicar el parche, ya que el cambio puede romper consultas existentes.

Solución

Actualizar de forma inmediata a las versiones corregidas:

Versión afectada	Versión corregida	Enlace de descarga
Django 5.2.x (hasta 5.2.16)	**5.2.17**	https://www.djangoproject.com/download/
Django 6.0.x (hasta 6.0.7)	**6.0.8**	https://www.djangoproject.com/download/

Actualización vía pip:

pip install «django>=5.2.17» # para rama 5.2

pip install «django>=6.0.8» # para rama 6.0

Commit de corrección (rama 5.2):
https://github.com/django/django/commit/115ffd0463a765ab1cc93de18e94b5459b8a300e

Información adicional:

- **Security Online — CVE-2026-15307:** https://securityonline.info/django-vulnerability-cve-2026-15307-rce/securityonline
- **Debian Security Tracker — CVE-2026-15307:** https://security-tracker.debian.org/tracker/CVE-2026-15307security-tracker.debian
- **Django — Página oficial de descargas:** https://www.djangoproject.com/download/
- **Django — Archivo de alertas de seguridad:** https://docs.djangoproject.com/en/6.0/releases/security/
- **GitHub commit fix (5.2.17):** https://github.com/django/django/commit/115ffd0463a765ab1cc93de18e94b5459b8a300e