



网络安全预警通报

2026 年第 7 期（总第 65 期）

西安交通大学网络信息中心 2026 年 07 月 21 日

【预警类型】严重预警

【预警内容】

WordPress Core 未授权远程代码执行漏洞 (CVE-2026-60137) 高危风险通报

一、漏洞概述

近期，安全研究人员披露了 WordPress Core 组件中的一个严重未授权远程代码执行漏洞 (CVE-2026-60137, 又称 “wp2shell”)。该漏洞影响 WordPress 核心组件，攻击者无需身份认证即可通过 REST API 批处理接口触发漏洞，实现 SQL 注入，并进一步创建管理员账户、上传恶意文件，最终获取服务器控制权限。

WordPress 是一款基于 PHP 开发的开源内容管理系统 (CMS)，目前被广泛应用于企业门户网站、新闻发布系统、个人博客、电子商务平台等场景。由于 WordPress 部署范围广、互联网暴露资产数量庞大，该漏洞可能成为攻击者批量攻击网站的重要入口。

该漏洞存在于 WordPress REST API 批处理接口（/wp-json/batch/v1）。由于 serve_batch_request_v1()函数在处理批量请求时，对 URL 路径解析结果及参数校验数组处理异常，导致请求路由发生混淆。攻击者可利用构造的恶意请求绕过接口校验，将特殊参数传递至 WP_Query 查询逻辑中，触发未授权 SQL 注入。

攻击者成功利用该漏洞后，可进一步通过数据库操作创建管理员账号，并结合插件上传、主题修改等功能写入恶意代码，实现远程代码执行，最终完全控制目标 WordPress 站点服务器。

该漏洞具备以下特点：

- （1）无需身份认证即可利用；
- （2）攻击复杂度低，远程即可触发；
- （3）漏洞利用链完整，可由 SQL 注入进一步升级为服务器控制；
- （4）已有公开 PoC 及利用代码，存在被自动化攻击风险。

二、漏洞详情

1.技术原理

漏洞编号	CVE-2026-60137
漏洞名称	WordPress Core 未授权远程代码执行漏洞
漏洞类型	SQL 注入/远程代码执行
漏洞等级	严重
CVSS 评分	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
利用方式	远程利用
利用复杂度	低

PoC 情况 已公开

产生原因：

漏洞产生于 WordPress REST API 批处理功能处理请求过程中的逻辑缺陷。

WordPress REST API 提供批量请求处理接口/wp-json/batch/v1，用于一次性执行多个 REST API 请求。在处理批量请求时，函数 `serve_batch_request_v1()` 会解析请求路径，并根据匹配结果调用对应接口处理程序。

由于漏洞代码中用于路径匹配的 `$matches` 数组与用于参数验证的 `$validation` 数组存在异常对应关系，当攻击者构造特殊格式请求路径时，可导致路由解析结果错位，使攻击请求进入非预期处理流程，从而绕过原有的方法限制及参数校验。

攻击者随后可利用 `author_exclude` 参数，将恶意 SQL 语句注入 WordPress 查询逻辑中的 `author__not_in` 字段，由于参数未经有效过滤，最终导致数据库查询语句被篡改，实现未授权 SQL 注入。

进一步地，攻击者可结合 WordPress 内部功能实现攻击链扩展，包括：

利用 SQL 注入伪造文章数据；

操纵 oEmbed 缓存数据；

修改 Customizer 配置；

未授权创建管理员账号；

通过插件上传或文件写入功能部署 WebShell。

最终实现远程代码执行，获得服务器控制权限。

2.利用条件

攻击者实施漏洞利用需满足以下条件：

- 目标部署 WordPress 网站，并启用了 REST API 功能；
- 目标 WordPress 版本处于受影响范围；
- 攻击者能够访问目标网站 HTTP 服务；
- 目标系统未安装官方安全更新；
- REST API 批处理接口未进行访问限制。

三、漏洞影响范围

1.受影响版本

目前确认受影响的 WordPress 版本包括：

WordPress 6.9.0 至 6.9.4 版本；

WordPress 7.0.0 至 7.0.1 版本。

2.威胁严重性

漏洞属于严重级别远程代码执行漏洞，攻击者无需账号权限即可完成攻击，CVSS 评分达到 9.8。

漏洞成功利用后，攻击者可能实施以下攻击行为：

- 创建非法管理员账户，实现长期控制；
- 上传 WebShell 或恶意插件，执行任意服务器命令；
- 窃取网站数据库中的用户信息、业务数据；
- 篡改网站内容，发布恶意信息；
- 进一步入侵服务器内部网络，开展横向攻击；
- 部署勒索软件，影响业务系统正常运行。

由于 WordPress 网站通常直接暴露于互联网，且大量站点采用默认 REST API 配置，因此该漏洞具有较高攻击价值。随着 PoC 公开，预计后续可能出现针对该漏洞的大规模扫描和自动化攻击活动。

四、处置建议

1.官方修复方案

WordPress 官方已发布安全更新修复该漏洞，建议受影响单位立即升级至安全版本：

升级至 WordPress 7.0.2；