在 WordPress 中，REST API 的 /batch/v1 端点在处理批量请求时存在路由混淆缺陷（CVE-2026-63030）。serve_batch_request_v1() 函数在处理子请求时，构建了 $matches（匹配的处理程序）和 $validation（验证结果）两个并行数组，但当子请求路径在 wp_parse_url() 解析失败时，该子请求仅被追加到 $validation 数组而未进入 $matches 数组，导致数组偏移错位，使得后续子请求被错误地分配到其他处理程序。攻击者可通过构造嵌套批量请求，在内层 POST 请求中携带 GET 参数（如 author_exclude），该参数在 WP_Query 中未经净化便被拼接到 SQL 语句中，形成布尔型和时间型盲注（CVE-2026-60137）。利用该注入可读取管理员密码哈希，破解后通过插件上传功能实现任意代码执行。

目前该漏洞的漏洞细节、POC 已公开。

## 风险等级

高风险

漏洞风险
未经身份验证的远程攻击者利用该漏洞可读取数据库任意内容，获取管理员密码哈希，进而通过插件上传实现远程代码执行，完全控制目标 WordPress 站点等危害。

影响版本
6.8.0 <= WordPress <= 6.8.5
6.9.0 <= WordPress <= 6.9.4
7.0.0 <= WordPress <= 7.0.1

## 安全版本

WordPress >= 6.8.6
WordPress >= 6.9.5
WordPress >= 7.0.2

## 检测方法

1. 检查所使用的软件或者补丁的版本
2. 使用 wp2shell.com 在线检测工具扫描 WordPress 站点是否存在该漏洞。

## 修复建议

1. 官方已发布漏洞补丁及修复版本，请评估业务是否受影响后，升级至安全版本
https://github.com/WordPress/wordpress-develop/tags
2. 缓解措施：
(1) 如无法升级，在边缘设备（如 WAF、反向代理）拦截对 /wp-json/batch/v1 和 /?rest_route=/batch/v1 的请求；
(2) 安装 Disable WP REST API 插件，禁用未认证用户对 WordPress REST API 的访问，但存在一定风险，可能会破坏现有功能；
(3) 使用 Searchlight Cyber 安全研究团队提供的自定义插件（详见 wp2shell.com），将其放入 wp-content/plugins/disable-batch-api-for-unauth.php 并启用，以强制 REST Batch API 需身份验证；
(4) 审计服务器日志，排查对 /batch/v1 端点的异常批量请求模式。