CYBER ADVISORY

Monday, July 20, 2026 **CAL-CSIC-202607-A-009**

Chained Vulnerabilities Impacting WordPress Core

SQL Injection	Full System Compromise	Remote Code Execution	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two vulnerabilities that can be chained to achieve remote code execution against WordPress Core installations. CVE-2026-63030 is a critical REST API Batch-Route Confusion Remote Code Execution (RCE) Vulnerability that carries a CVSS 3.1 score of 9.8.[1] CVE-2026-60137 is an SQL Injection vulnerability that normally carries a CVSS 3.1 score of 5.9. When utilized in conjunction with CVE-2026-63030, the CVSS 3.1 score is raised to 9.1.[2]

When these two vulnerabilities are chained together (dubbed WP2Shell), it enables an unauthenticated attacker to reach the REST API batch endpoint at */wp-json/batch/v1* to achieve remote code execution. Successful exploitation allows the attacker to fully compromise the targeted site to exfiltrate data, escalate privileges, remote code execution, and persistence. A publicly available proof-of-concept is available, and in-the-wild exploitation is currently being observed by multiple independent security firms.[3]

WordPress have acknowledged both vulnerabilities and have issued security updates to patch this exploit.

The Cal-CSIC recommends following the WordPress' update guidance as soon as possible. If patching is not immediately possible, there are three temporary workarounds:

1. Install a plugin that blocks unauthenticated users from accessing the REST API.
2. Block **/wp-json/batch/v1** and **?rest_route=/batch/v1** at the web application firewall (WAF) level and ensure both patterns are covered.[4]
3. Deploy a custom PHP plugin available on wp2shell.com that restricts unauthenticated access to the batch endpoint specifically.[5]

For additional details regarding the exploit, please use these links:

WP2Shell FAQs: WordPress wp2shell (CVE-2026-63030): CISO FAQ & Fix

WordPress 7.0.2 Release: https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

Affected Product and Version

WordPress Branch	Affected Version	Fixed Version	Applicable CVE
6.8.x	6.8.0-6.8.5	6.8.6	CVE-2026-60137
6.9.x	6.9.0-6.9.4	6.9.5	CVE-2026-63030 CVE-2026-60137
7.0.x	7.0.0-7.0.1	7.0.2	CVE-2026-63030 CVE-2026-60137
7.1 beta	7.1 beta	7.1 beta2	CVE-2026-63030 CVE-2026-60137

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-63030 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-63030; accessed 20 July 2026
[2] NVD; "CVE-2026-60137 Detail"; https://nvd.nist.gov/vuln/detail/cve-2026-60137; accessed 20 July 2026
[3] SOCRadar; "WordPress wp2shell Vulnerability"; https://socradar.io/blog/wp2shell-wordpress-rce-cve-2026-63030/#:~:text=This%20is%20the%20entry%20point%20rated%20Critical,GitHub%20advisory%20GHSA%2Dff9f%2Djf42%2D662q%2C%20introduced%20in%20WordPress%206.9.; accessed 20 July 2026
[4] Tenable; "wp2shell (CVE-2026-63030, CVE-2026-60137): Frequently asked questions about remote code execution chain in WordPress Core"; https://www.tenable.com/blog/wp2shell-cve-2026-63030-cve-2026-60137-frequently-asked-questions-about-remote-code-execution; accessed 20 July 2026
[5] SearchlightCyber; "wp2shell Pre Authentication RCE in WordPress Core"; https://wp2shell.com/; accessed 20 July 2026