New WordPress Core Flaw Allows Unauthenticated Code Execution

Description

An anonymous HTTP request can run code on a WordPress site. This issue affects software versions 6.9 and 7.0, which are at risk until the recent patch. WordPress has released updates 6.9.5 and 7.0.2 to fix the problem.

The flaw, known as wp2shell, consists of two bugs with CVE IDs. CVE-2026-63030 relates to a mistake in the REST API, while CVE-2026-60137 is a SQL injection in WordPress. Together, these bugs can allow an anonymous user to execute code on the site.

Adam Kues from Assetnote discovered the batch-route bug and reported it through WordPress's HackerOne program. Researchers have published details about the attack, which requires no prior conditions to be triggered. The injection flaw has been noted separately by other contributors.

Not all versions have the same vulnerabilities. The SQL injection affects versions up to 6.8.5, while the batch-route issue only appears from version 6.9 onwards. Therefore, users should be aware of which version they are running.

WordPress has not confirmed if automatic updates will reach sites that have switched off this feature. Users should check their version to ensure they are protected. The issue impacts a large number of sites, with over 500 million running WordPress globally.

To protect against this bug until an update is made, users should consider blocking certain API routes or completely disabling the REST API.

Vocabulary List:

1. **anonymous** /əˈnɑnəməs/ (adjective): not using a real or known name
2. **vulnerabilities** /ˌvʌlnərəˈbɪlətiz/ (noun): weak parts that can be used to harm
3. **injection** /ɪnˈdʒɛkʃən/ (noun): adding harmful code into software or database
4. **execute** /ˈɛksɪˌkjuːt/ (verb): to run a program or command
5. **patch** /pætʃ/ (noun): a small update that fixes software problems
6. **triggered** /ˈtrɪgərd/ (verb): caused something to start or happen

Comprehension Questions

Multiple Choice

1. What is the code name of the flaw that affects WordPress versions 6.9 and 7.0?

   Option: wp2shell
   Option: batch-route
   Option: CVE-2026-63030
   Option: CVE-2026-60137

2. Which user discovered the batch-route bug?

   Option: Adam Kues
   Option: WordPress Team
   Option: HackerOne
   Option: Assetnote

3. What is the highest affected version for SQL injection vulnerabilities?

   Option: 6.9
   Option: 6.9.5
   Option: 6.8.5
   Option: 7.0

4. What is the version number of the recent patch released by WordPress?

   Option: 6.9.5
   Option: 7.0.2
   Option: 6.8.5
   Option: 7.1

5. How many WordPress sites are running globally?

   Option: 100 million
   Option: 200 million
   Option: 500 million
   Option: 1 billion

6. Which CVE ID relates to the SQL injection vulnerability?

   Option: CVE-2026-63030
   Option: CVE-2026-60137
   Option: CVE-2023-12345
   Option: CVE-2023-67890

True-False

7. The batch-route issue affects WordPress versions below 6.9.

8. WordPress has confirmed that automatic updates will apply to all sites.

9. An anonymous user can execute code on a WordPress site due to this vulnerability.

10. The injection flaw requires prior conditions to be triggered.

11. Adam Kues reported the bug through WordPress's HackerOne program.

12. All versions of WordPress have the same vulnerabilities related to wp2shell.

Gap-Fill

13. WordPress versions affected by the flaw include 6.9 and _____ .

14. The flaw consists of two bugs with CVE IDs, one of which is CVE-2026-_____ .

15. To protect against the bug, users should consider blocking certain API _____ .

16. The SQL injection affects versions up to 6.8_____ .

17. The batch-route bug requires _____ conditions to be triggered.

18. Over _____ million sites run WordPress globally.

Answer

Multiple Choice: 1. wp2shell 2. Adam Kues 3. 6.8.5 4. 6.9.5 5. 500 million 6. CVE-2026-60137
True-False: 7. False 8. False 9. True 10. False 11. True 12. False
Gap-Fill: 13. 7.0 14. 63030 15. routes 16. 5 17. no 18. 500

CATEGORY

1. Sci/Tech - LEVEL3

POST TAG

1. B1

2. ESL learning
3. esl news
4. Level 3
5. new wp2shell
6. unauthenticated attackers
7. WordPress Core

Tags

1. B1
2. ESL learning
3. esl news
4. Level 3
5. new wp2shell
6. unauthenticated attackers
7. WordPress Core

Date Created
2026/07/18
Author
aimeeyoung99