Vulnerabilità critica WordPress "WP2Shell" (RCE) – Aggiornamento immediato consigliato

Christian Cantinelli - 2026-07-20 - Applicazione CMS

È stata divulgata una **vulnerabilità critica nel core di WordPress**, identificata come **WP2Shell**, che può consentire ad un attaccante remoto **non autenticato** di compromettere completamente un sito web.

La vulnerabilità interessa **il core di WordPress** e **non dipende da plugin o temi vulnerabili**: anche un'installazione standard di WordPress può risultare esposta.

Un attaccante può sfruttare una catena di vulnerabilità per ottenere l'esecuzione di codice arbitrario (Remote Code Execution - RCE), con possibili conseguenze quali:

- installazione di malware o web shell;
- modifica o cancellazione dei contenuti del sito;
- furto di dati presenti nel database;
- utilizzo del sito per campagne di spam o phishing;
- compromissione dell'intero account hosting.

Poiché è già stato pubblicato un **Proof of Concept (PoC)**, è prevedibile un rapido aumento dei tentativi di sfruttamento automatico da parte degli attaccanti.

Versioni interessate

Vulnerabili alla Remote Code Execution (RCE)

Sono vulnerabili le seguenti versioni del core WordPress:

- **6.9.0 - 6.9.4**
- **7.0.0 - 7.0.1**

Versioni corrette:

- **6.9.5**
- **7.0.2**

Vulnerabili alla SQL Injection

Le versioni:

- **6.8.0 - 6.8.5**

sono interessate da una vulnerabilità SQL Injection, corretta nella versione:

- **6.8.6**

Pur non essendo interessate dalla catena completa WP2Shell, è comunque fortemente consigliato l'aggiornamento.

Cosa fare

L'aggiornamento del core di WordPress rappresenta l'unica soluzione definitiva.

Si raccomanda di aggiornare il prima possibile alla versione corretta corrispondente al proprio ramo di sviluppo:

Versione installata	Aggiornare almeno a
6.8.x	6.8.6
6.9.x	6.9.5
7.0.x	7.0.2

Prima di procedere è sempre consigliabile verificare la disponibilità di un backup recente.

Mitigazione temporanea tramite .htaccess

Qualora non fosse possibile aggiornare immediatamente WordPress, è possibile ridurre temporaneamente il rischio bloccando l'accesso all'endpoint REST API utilizzato dalla vulnerabilità.

Inserire le seguenti direttive nel file `.htaccess` presente nella cartella principale dell'installazione WordPress, **prima** della sezione racchiusa tra:

```
# BEGIN WordPress
...
# END WordPress
```

Utilizzare le seguenti regole:

```
# Mitigazione temporanea vulnerabilità WordPress WP2Shell
<IfModule mod_rewrite.c>
RewriteEngine On

# Blocca /wp-json/batch/v1 e gli eventuali percorsi subordinati
RewriteCond %{REQUEST_URI} ^/wp-json/batch/v1(?:/|$) [NC]
RewriteRule ^ - [F,L]

# Blocca anche index.php?rest_route=/batch/v1
RewriteCond %{QUERY_STRING} (^|&)rest_route=(%2F|/)?batch(%2F|/)v1(?:%2F|/|&|$) [NC]
RewriteRule ^ - [F,L]
</IfModule>
```

In presenza di un'installazione WordPress collocata in una sottocartella, ad esempio:

```
https://www.example.com/blog/
```

il controllo sul percorso deve includere anche la sottocartella:

```
RewriteCond %{REQUEST_URI} ^/blog/wp-json/batch/v1(?:/|$) [NC]
RewriteRule ^ - [F,L]
```

Verifica del blocco

Dopo aver applicato le regole, è possibile verificarne il funzionamento con:

```
curl -I https://www.example.com/wp-json/batch/v1
```

e:

```
curl -I "https://www.example.com/index.php?rest_route=/batch/v1"
```

In entrambi i casi il server dovrebbe restituire:

```
HTTP/1.1 403 Forbidden
```

È consigliabile provare anche la variante con il percorso codificato:

```
curl -I "https://www.example.com/index.php?rest_route=%2Fbatch%2Fv1"
```

Anche questa richiesta deve ricevere una risposta `403 Forbidden`.

Possibili incompatibilità

Il blocco è circoscritto all'endpoint REST batch e non disabilita completamente la REST API di WordPress. Tuttavia, potrebbe interferire con plugin, temi o integrazioni che utilizzano specificamente la funzionalità di elaborazione batch.

Dopo l'applicazione è quindi opportuno verificare almeno:

- il funzionamento dell'editor a blocchi;
- la gestione degli ordini e del back office di WooCommerce;
- eventuali applicazioni o servizi esterni collegati tramite REST API;
- le funzionalità di plugin che effettuano richieste multiple tramite REST API.

> **Importante:** questa configurazione costituisce esclusivamente una mitigazione temporanea. Non corregge la vulnerabilità presente nel core di WordPress e deve essere rimossa dopo aver installato una versione aggiornata e non vulnerabile.

La soluzione definitiva rimane l'aggiornamento immediato almeno a WordPress **6.8.6**, **6.9.5** o **7.0.2**, in base al ramo attualmente utilizzato.