SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

Vulnerabilități exploatate activ în WordPress Core

CVE-2026-63030 · CVE-2026-60137 · lanțul „wp2shell”

Executare de cod la distanță, neautentificată

Raport tehnic | STISC

26.08.2026

PUBLIC · TLP:CLEAR

Raport tehnic de securitate

SUMAR

Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) informează despre două vulnerabilități în WordPress Core, CVE-2026-63030 și CVE-2026-60137, exploatate activ. Combinate în lanțul „wp2shell”, acestea permit compromiterea completă a unor versiuni WordPress expuse public, fără autentificare și fără interacțiunea utilizatorului. Actualizarea imediată și investigația retrospectivă sunt obligatorii.

Câmp	Evaluare
Produs afectat	WordPress Core
Identificatori	CVE-2026-63030 și CVE-2026-60137
Nivel operațional	**CRITIC — exploatare activă / CISA KEV**
Vector	Rețea, fără autentificare și fără interacțiunea utilizatorului
Impact	SQL injection, creare administrator și execuție PHP arbitrară
Data raportului	26.08.2026

CONCLUZIE EXECUTIVĂ

Instanțele WordPress 6.9.0–6.9.4 și 7.0.0–7.0.1 trebuie considerate expuse la compromitere completă dacă REST API este accesibil. CVE-2026-63030 permite confuzia handlerelor din endpoint-ul batch, iar CVE-2026-60137 introduce SQL prin parametrul public author_exclude. Lanțul poate crea un administrator și permite încărcarea unui plugin malițios pentru execuție PHP.

1. Rezumat și evaluarea riscului

La 17 iulie 2026, WordPress a publicat versiunile 7.0.2, 6.9.5 și 6.8.6 pentru remedierea a două vulnerabilități în WordPress Core. Versiunile 6.9 și 7.0 sunt afectate de ambele probleme, iar ramura 6.8 este afectată numai de vulnerabilitatea SQL injection. WordPress a activat actualizări forțate pentru versiunile afectate, însă administratorii trebuie să confirme explicit versiunea instalată și integritatea site-ului.

Ambele CVE au fost adăugate în catalogul CISA Known Exploited Vulnerabilities la 21 iulie 2026. Termenul CISA pentru CVE-2026-63030 a fost 24 iulie 2026, iar pentru CVE-2026-60137 — 4 august 2026. La data prezentului raport, ambele termene sunt depășite; orice activ vulnerabil necesită escaladare imediată.

CVE	Severitate publicată	CWE	Exploatare	Rol în lanț
CVE-2026-63030	WPScan 9,8 Critic; CISA-ADP 7,5 Ridicat	CWE-436	Activă; PoC public	Confuzie rută/handler; face SQLi accesibilă pre-auth
CVE-2026-60137	WPScan 5,9 Mediu; CISA-ADP 9,1 Critic	CWE-89	Activă; PoC public	SQL injection în WP_Query; divulgare/modificare DB

2. Fișă tehnică — CVE-2026-63030

Câmp tehnic	Evaluare
Condiția necesară pentru exploatare	WordPress 6.9.0–6.9.4 sau 7.0.0–7.0.1; endpoint REST Batch accesibil prin /wp-json/batch/v1 ori rest_route=/batch/v1; solicitări HTTP POST anonime permise. Pentru calea RCE descrisă public, mediul fără cache persistent extern este cel mai direct exploatabil; prezența Redis/Memcached nu trebuie considerată remediere.
Descriere succintă	Confuzie de rutare/interpretare în procesorul REST API batch. O subcerere este validată față de o rută, dar poate fi executată de handlerul altei rute, permițând ocolirea validării și a restricțiilor așteptate.
CVSS v3.1	WPScan/CNA: 9,8 Critic — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. CISA-ADP: 7,5 Ridicat — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N. NVD: scor propriu indisponibil la 26.08.2026.
Tipul vulnerabilității	CWE-436 — Interpretation Conflict / REST API route confusion; slăbiciune logică în corelarea rutelor validate cu handler-ele executate.
Mod de exploatare	Remote, prin cereri POST JSON special construite către endpoint-ul batch. Nu necesită cont valid și nu necesită interacțiunea utilizatorului.
Cauza	WP_REST_Server::serve_batch_request_v1() gestionează validarea și potrivirile de rută în structuri paralele. Când wp_parse_url() eșuează pentru o cale invalidă, este înregistrată eroarea de validare, dar nu este adăugat un element corespondent în lista de potriviri. Indexarea se desincronizează, iar cererile următoare pot primi handlerul greșit.
Metode de exploatare	Subcereri batch imbricate; inserarea unei căi nevalide care provoacă desincronizarea; dirijarea unei cereri către /wp/v2/posts fără validarea normală; combinare cu CVE-2026-60137 pentru UNION-based SQLi, creare de administrator și RCE prin plugin PHP.
Versiuni afectate	WordPress 6.9.0–6.9.4 și 7.0.0–7.0.1. Versiunile anterioare 6.9 nu sunt afectate de această vulnerabilitate. Beta 7.1 anterioară beta2 a fost afectată.
Versiuni remediate	WordPress 6.9.5, 7.0.2 și 7.1 beta2 sau orice versiune ulterioară suportată care include remedierea.
Consecințe	Ocolirea validării REST; acces la handler-e neautorizate; SQL injection pre-auth în combinație cu CVE-2026-60137; creare cont administrator; instalare plugin malițios; execuție PHP arbitrară; compromiterea confidențialității, integrității și disponibilității site-ului.
Detectare și monitorizare	Monitorizarea POST către toate variantele batch/v1; corpuri JSON cu requests imbricate, path „///”, /wp/v2/posts și author_exclude; procese shell/utilitare lansate de php-fpm/httpd/nginx; conturi administrator noi; fișiere PHP noi în wp-content/plugins, mu-plugins sau uploads.

3. Fișă tehnică — CVE-2026-60137

Câmp tehnic	Evaluare
Condiția necesară pentru exploatare	WordPress 6.8.0–6.8.5, 6.9.0–6.9.4 sau 7.0.0–7.0.1. Izolat, este necesar ca o temă/un plugin ori un flux autorizat să transmită input neîncredere către author__not_in. În lanțul wp2shell pe 6.9/7.0, CVE-2026-63030 o face accesibilă unui atacator neautentificat prin REST Batch API.
Descriere succintă	Sanitizare insuficientă a parametrului intern author__not_in din WP_Query. O valoare scalară controlată de atacator poate ajunge în construcția interogării SQL în locul unui tablou de identificatori numerici.
CVSS v3.1	WPScan/CNA: 5,9 Mediu — AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N. CISA-ADP: 9,1 Critic — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N. NVD: scor propriu indisponibil la 26.08.2026.
Tipul vulnerabilității	CWE-89 — Improper Neutralization of Special Elements used in an SQL Command („SQL Injection”).
Mod de exploatare	Parametrul REST public author_exclude este mapat la author__not_in. Un șir malițios poate modifica interogarea WP_Query; în lanțul wp2shell se utilizează cereri batch imbricate și o tehnică UNION-based.
Cauza	Codul tratează author__not_in ca listă numerică și aplică sanitizarea adecvată numai formei așteptate. O valoare scalară ajunge necurățată în clauza SQL. Separarea dintre schema REST și interogarea internă eșuează atunci când route confusion ocolește validarea normală.
Metode de exploatare	Transmiterea author_exclude/author__not_in cu metacaractere SQL; UNION SELECT pentru obținerea de date sau injectarea unor rezultate sintetice; folosirea obiectelor WP_Post hidratate și a fluxurilor oEmbed/Customizer pentru escaladarea efectului până la crearea unui administrator.
Versiuni afectate	WordPress 6.8.0–6.8.5; 6.9.0–6.9.4; 7.0.0–7.0.1.
Versiuni remediate	WordPress 6.8.6, 6.9.5, 7.0.2 și 7.1 beta2 sau orice versiune ulterioară suportată care include remedierea.
Consecințe	Citirea datelor din baza WordPress, inclusiv hash-uri și date sensibile; manipularea rezultatelor interogărilor; modificarea stării aplicației; în combinație cu CVE-2026-63030 — preluare cont administrator și RCE.
Detectare și monitorizare	Căutarea parametrului extern author_exclude în trafic, nu doar author__not_in; secvențe URL-encoded asociate cu „UNION SELECT”, comentarii SQL și CONCAT/HEX; răspunsuri REST neobișnuit de mari; activitate DB anormală; conturi/roluri și pluginuri nou create.

4. Descrierea tehnică a lanțului de atac „wp2shell”

1. Descoperirea și enumerarea țintei. Atacatorul identifică o instanță WordPress și verifică accesul la REST API, inclusiv ruta /wp-json/batch/v1 și variantele rest_route.
2. Declanșarea confuziei de rută. O cerere batch conține o cale intenționat invalidă și cereri ulterioare valide. Eșecul de parsare desincronizează lista validărilor de lista handlerelor potrivite.
3. Ocolirea validării. O subcerere ulterioară este executată de alt handler decât cel față de care a fost validată, făcând accesibilă pre-auth calea către WP_Query.
4. SQL injection. Parametrul HTTP author_exclude ajunge la argumentul intern author__not_in ca șir scalar și alterează interogarea SQL. Activitatea observată folosește injecție de tip UNION.
5. Escaladarea în aplicație. Cercetarea publică descrie abuzul hidratării obiectelor WP_Post, cache-ului oEmbed și salvărilor imbricate pentru a manipula starea aplicației și a crea un utilizator cu rol administrator.
6. Execuția codului. Noul cont administrator poate instala sau activa un plugin PHP malițios. Codul rulează cu identitatea procesului web/PHP și poate iniția comenzi shell, descărca unelte și modifica fișierele site-ului.

LIMITARE IMPORTANTĂ

Niciuna dintre vulnerabilități, analizată izolat, nu descrie întregul rezultat RCE pre-auth. Riscul critic rezultă din combinarea lor pe WordPress 6.9/7.0. Cache-ul persistent extern poate modifica calea de exploatare publicată, dar nu repară defectele și nu reduce obligația de actualizare.

5. Condiții critice pentru exploatare

1. Instanță WordPress într-un interval vulnerabil și accesibilă prin HTTP/HTTPS.
2. REST API activ și endpoint-ul batch/v1 accesibil unui client neautentificat.
3. Lipsa patch-ului WordPress Core, inclusiv în imagini container, copii de staging și site-uri secundare uitate.
4. Pentru calea completă observată public: WordPress 6.9/7.0 și condiții de cache compatibile cu lanțul; instalarea implicită fără cache persistent extern este expusă.
5. Lipsa unei reguli WAF care inspectează corpul JSON și blochează atât ruta standard, cât și variantele rest_route.
6. Permisiunea procesului PHP de a modifica wp-content/plugins sau alte directoare executabile amplifică impactul post-compromitere.

6. Versiuni afectate și remediate

Ramură	Stare	Vulnerabilitate aplicabilă	Acțiune minimă
< 6.8	Neafectată de aceste două CVE	Niciuna	Menținere pe o versiune suportată și actualizată
6.8.0–6.8.5	Vulnerabilă	CVE-2026-60137 (SQLi)	Actualizare la minimum 6.8.6
6.8.6	Remediată pentru aceste CVE	—	Verificare integritate și plan de upgrade suportat
6.9.0–6.9.4	Critic vulnerabilă	Ambele; lanț RCE pre-auth	Actualizare la minimum 6.9.5
6.9.5	Remediată pentru aceste CVE	—	Preferabil ultima versiune suportată
7.0.0–7.0.1	Critic vulnerabilă	Ambele; lanț RCE pre-auth	Actualizare la minimum 7.0.2
7.0.2+	Remediată pentru aceste CVE	—	Aplicarea tuturor actualizărilor ulterioare

7. Detectare și monitorizare

7.1. Nivel HTTP / reverse proxy / WAF

Prioritatea este corelarea rutelor batch cu parametrul author_exclude și indicatori SQL. Jurnalele web standard nu includ, de regulă, corpul POST; pentru confirmarea payload-ului sunt necesare logurile WAF/reverse proxy cu request body sau captură de rețea autorizată.

```
# Nginx/Apache: rută batch în jurnale text
rg -n -i '(/wp-json/batch/v1|rest_route=(%2F|/)batch(%2F|/)v1)' /var/log/nginx/access.log /var/log/apache2/access.log

# Jurnale comprimate
zgrep -Eai '(/wp-json/batch/v1|rest_route=(%2F|/)batch(%2F|/)v1)' /var/log/nginx/access.log.*.gz /var/log/apache2/access.log.*.gz
```

Indicatori de fidelitate ridicată în request body: requests imbricat, path cu „///”, /wp/v2/posts, author_exclude și tokenuri SQL encodate/dezencodate precum UNION SELECT, CONCAT, HEX, comentarii „--” sau per_page=500. Un acces simplu la batch/v1 nu dovedește exploatarea, dar necesită triere.

7.2. Nivel WordPress și bază de date

```
# Versiune și integritatea fișierelor WordPress Core
wp core version --path=/var/www/html --extra
wp core verify-checksums --path=/var/www/html --include-root

# Administratori și data înregistrării
wp user list --path=/var/www/html --role=administrator \
  --fields=ID,user_login,user_email,user_registered,roles --format=table

# Pluginuri și starea lor
wp plugin list --path=/var/www/html --fields=name,status,version,update --format=table

# Fișiere PHP modificate după publicarea vulnerabilităților
find /var/www/html/wp-content -type f \
  \( -name '*.php' -o -name '*.phtml' -o -name '*.phar' \) \
  -newermt '2026-07-17' -ls
```

7. Investigați administratori necunoscuți sau creați după 17.07.2026; corelați cu autentificările și IP-ul sursă.
8. Comparați pluginurile active cu inventarul aprobat; verificați directoare cu denumiri aleatorii, fișiere principale noi și modificări în functions.php.
9. Examinați wp_options pentru active_plugins, cron și valori serializate modificate neautorizat.
10. Verificați logurile MySQL/MariaDB sau audit plugin pentru SELECT-uri anormale generate de WP_Query și acces neobișnuit la tabelele *_users și *_usermeta.

7.3. Nivel sistem și procese

```
# Procese și conexiuni active ale serviciilor web/PHP
ps -eo pid,ppid,user,lstart,cmd --forest | rg -i '(php-fpm|php-cgi|apache2|httpd|nginx|bash|sh|curl|wget)'
ss -plant | rg -i '(php|apache|httpd|nginx)'

# Fișiere executabile/scripturi schimbate în zonele WordPress
find /var/www/html -xdev -type f -newermt '2026-07-17' -printf '%TY-%Tm-%Td %TH:%TM %u %m %p\n' | sort
```

Semnale post-exploatare: php-fpm/httpd/nginx care lansează sh, bash, curl, wget, python, perl, nc sau socat; scriere de PHP în uploads; conexiuni externe inițiate de procesele web; modificarea .htaccess, wp-config.php, cron, systemd sau cheilor SSH.

8. IOC, IOA și TTP

8.1. Indicatori de rețea și aplicație

Indicator	Nivel de încredere	Interpretare / acțiune
/wp-json/batch/v1; /index.php?rest_route=/batch/v1; /?rest_route=/batch/v1	Mediu	Rută de atac; accesul legitim este posibil. Corelați cu POST, nested requests și author_exclude.
author_exclude + UNION SELECT / CONCAT / HEX / comentarii SQL	Ridicat	Indicator direct al tentativei SQLi wp2shell; blocați și investigați sursa/ținta.
path „///” în subcereri JSON batch	Ridicat	Declanșator observat pentru eroarea de parsare și desincronizare.
185.242.3.238	Ridicat	F5 Labs a capturat un payload wp2shell complet de la această adresă. Căutați retrospectiv; reputația IP se poate schimba.
47.129.160.40; 94.159.96.62; 207.180.249.59; 13.140.128.125	Scăzut–Mediu	Surse cu volum mare către rute batch în telemetria F5; payload wp2shell neconfirmat pentru aceste IP-uri. Nu blocați exclusiv pe baza listei.
User-Agent Chrome/126 Linux x86_64	Scăzut	Observat în payload-ul capturat; ușor de falsificat, util numai în corelare.

8.2. Indicatori de compromitere pe gazdă

1. Cont administrator WordPress necunoscut sau creat fără tichet aprobat.
2. Plugin activat/instalat recent, mai ales cu nume aleator, fișier PHP unic sau funcții de execuție/încărcare.
3. PHP în wp-content/uploads ori mu-plugins care nu corespunde baseline-ului.
4. Procese sh/bash/curl/wget/python/nc cu părinte php-fpm, httpd, apache2 sau nginx.
5. Conexiuni outbound neobișnuite ale contului www-data/apache/nginx și modificări ale wp-config.php, .htaccess, cron/systemd sau cheilor SSH.
6. Eșec la wp core verify-checksums ori fișiere core suplimentare neexplicate.

8.3. Mapare MITRE ATT&CK

ID	Tehnică	Utilizare în scenariul wp2shell
T1595.002	Active Scanning: Vulnerability Scanning	Enumerarea WordPress, REST API și a endpoint-ului batch.
T1190	Exploit Public-Facing Application	Exploatarea route confusion + SQL injection pe aplicația web publică.
T1136	Create Account	Crearea unui utilizator WordPress cu rol administrator.
T1078	Valid Accounts	Autentificarea cu administratorul creat/compromis.
T1505.003	Server Software Component: Web Shell	Posibilă încărcare a unui plugin/webshell PHP pentru execuție persistentă.
T1059.004	Command and Scripting Interpreter: Unix Shell	Comenzi lansate de procesul web după obținerea RCE.
T1105	Ingress Tool Transfer	Descărcarea de payload-uri/unelte prin curl, wget sau utilitare similare.

9. Remediere și reducerea riscului

9.1. Acțiune prioritară — actualizare

```
# Din directorul WordPress, cu backup verificat și fereastră aprobată
wp core version --extra
wp db export /cale-securizata/wordpress-pre-update-$(date +%F-%H%M).sql
wp core update
wp core update-db
wp core verify-checksums --include-root
wp core version --extra
```

Dacă politica impune menținerea ramurii, pragurile minime sunt 6.8.6, 6.9.5 și 7.0.2. Recomandarea practică este ultima versiune WordPress suportată și compatibilă, împreună cu actualizarea pluginurilor, temelor, imaginii container și a tuturor clonelor/staging-urilor.

9.2. Măsuri temporare când patch-ul nu poate fi aplicat imediat

Măsurile temporare reduc suprafața, dar nu înlocuiesc actualizarea. Blocați anonim endpoint-ul batch atât prin ruta standard, cât și prin parametrul rest_route și activați protecțiile SQLi cu inspecția corpului JSON.

```
# Nginx — exemplu de blocare temporară
location = /wp-json/batch/v1 { return 403; }
location = /wp-json/batch/v1/ { return 403; }
if ($arg_rest_route ~* '^/batch/v1/?$') { return 403; }

# Apache mod_rewrite — exemplu de blocare temporară
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/wp-json/batch/v1/?$ [NC,OR]
RewriteCond %{QUERY_STRING} (^|&)rest_route=(%2F|/)batch(%2F|/)v1/?(&|$) [NC]
RewriteRule ^ - [F,L]
```

Pentru Cloudflare Managed Ruleset, sursa oficială publică indică regulile: 1c060d3a371549219ee290d7ed933fcc (CVE-2026-60137) și 7dfb2bd4708d4b88b9911dc0550664b6 (CVE-2026-63030); în Free Ruleset: db003b39b7774859a8d588ce33697a1a și ebd3f2df15c74ddcbf6220c9b5ec246a. Confirmați că acțiunea este Block și că regulile sunt active.

9.3. Hardening după actualizare

7. Restricționați scrierea procesului web; wp-content/uploads nu trebuie să execute PHP. Limitați instalarea de pluginuri la fluxul administrativ aprobat.
8. Protejați wp-admin cu MFA, restricții de rețea/VPN unde este posibil și alertare la creare de utilizatori/roluri administrator.
9. Centralizați logurile WAF, web, WordPress audit, DB și Falcon; păstrați retenție care acoperă cel puțin perioada de la 17.07.2026.
10. Mențineți inventarul complet al domeniilor, subdomeniilor, containerelor și instanțelor de staging; verificați explicit imaginile neschimbate după redeploy.
11. Activați monitorizarea integrității pentru directoarele WordPress și baseline de hash-uri; separați backup-urile de contul serviciului web.

10. Constatări principale

1. CVE-2026-63030 și CVE-2026-60137 sunt exploatate activ și figurează în CISA KEV.
2. Lanțul complet afectează WordPress 6.9.0–6.9.4 și 7.0.0–7.0.1 și nu necesită pluginuri terțe, cont sau interacțiune.
3. Ramura 6.8.0–6.8.5 este afectată de SQL injection, dar nu de lanțul RCE descris pentru 6.9/7.0.
4. Parametrul observabil în traficul HTTP este author_exclude; author__not_in este denumirea internă WP_Query.

5. Actualizarea este remedierea principală; blocarea batch/v1 este numai măsură temporară.
6. Organizațiile trebuie să efectueze hunting retrospectiv și verificare de integritate chiar după patch, deoarece exploatarea a început rapid după publicare.

11. Surse

7. WordPress 7.0.2 Security Release
8. WordPress/GitHub Advisory — CVE-2026-63030
9. WordPress/GitHub Advisory — CVE-2026-60137
10. NIST NVD — CVE-2026-63030
11. NIST NVD — CVE-2026-60137
12. CISA Known Exploited Vulnerabilities Catalog
13. F5 Labs — wp2shell Captured Exploit Payload
14. Rapid7 — wp2shell Technical Overview
15. Akamai — Mitigating the wp2shell RCE Chain
16. Cloudflare — WAF protections for the WordPress vulnerabilities
17. VulnCheck — WP2Shell Vulnerabilities

Metodologie: informațiile de identificare, versiunile și remedierile au fost validate cu sursele WordPress/GitHub și NVD; exploatarea activă și telemetria au fost coroborate cu CISA, F5 Labs, Rapid7, Akamai, Cloudflare și VulnCheck. Interogările și comenzile de detecție reprezintă măsuri defensive și trebuie adaptate mediului tehnic.