Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

WordPress: Schwachstellen erlauben Remote Code Execution

BITS-H Nr. 2026-271984-1132, Version 1.1, 20.07.2026

Kritikalität*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Bitte prüfen Sie selbstständig, für welche Stellen in Ihrer Organisation die hier genannten Informationen relevant sind und leiten Sie das Schreiben entsprechend weiter – sofern die TLP-Einstufung dies zulässt.

Übersicht

Betroffenes Produkt	WordPress	**Gefährdung**	Aktive Ausnutzung
Betroffene Versionen	• 6.8.0-6.8.5 (nur von CVE-2026-60137 betroffen) • 6.9.0-6.9.4 • 7.0.0-7.0.1 • 7.1 beta	**Schutzmaßnahmen**	Patch + Workaround
Behebende Versionen	• 6.8.6 • 6.9.5 • 7.0.2 • 7.1 beta2 •	**CVEs**	• CVE-2026-60137 (CVSS 9.1/10) • CVE-2026-63030 (CVSS 7.5/10)

Sachverhalt

Am 17.07.2026 wurde seitens WordPress eine Aktualisierung bekannt gegeben [WP26], welche zwei Schwachstellen in der WordPress-Software behebt. WordPress ist ein weit verbreitetes Content Management System (CMS), insbesondere bei Blog-Betreibern und Webshops.

* 1 / Grau: Maßnahmen sollten in absehbarer Zeit erwogen werden. Keine wesentlichen Beeinträchtigungen zu erwarten.
2 / Gelb: Maßnahmen müssen zeitnah ergriffen werden. Temporäre Beeinträchtigungen des Regelbetriebs möglich.
3 / Orange: Maßnahmen müssen unverzüglich ergriffen werden. Massive Beeinträchtigung des Regelbetriebs möglich.
4 / Rot Maßnahmen müssen sofort ergriffen werden. Geschäftskritische Beeinträchtigung möglich.

Die beiden nun bekannt gewordenen Schwachstellen CVE-2026-60137 und CVE-2026-63030 ermöglichen in Kombination einem nicht-authentifizierten, entfernten Angreifer Code zur Ausführung zu bringen ("Remote Code Execution") und wurden auch als "wp2shell" getauft,.

Bei der Schwachstelle CVE-2026-60137 handelt es sich um eine fehlerhafte Sanitarisierung des Parameters "author__not_in parameter" bei WP_Query-Abfragen, welche zu SQL-Injection genutzt werden kann.

Die zweite Schwachstelle CVE-2026-63030 findet sich in der REST API von WordPress und erlaubt es in Kombination mit CVE-2026-60137, ohne Anmeldung am System, Code aus der Ferne zur Ausführung zu bringen ("Remote Code Execution").

Die Sicherheitsforscher bieten eine Webseite zur Prüfung auf Verwundbarkeit an - siehe [SC26b].

Mittlerweile ist ebenfalls ein weiterer Proof-of-Concept auf GitHub veröffentlicht worden - daher ist zeitnah mit aktiver Ausnutzung der Schwachstellen zu rechnen.

Update 1:

Im Laufe des Wochenendes sind PoCs veröffentlicht worden, die eine Ausnutzung der vollständigen Schwachstellenkette und damit Angriffe ohne Authentifizierung ermöglichen. Berichte über erste Ausnutzungen existieren ebenfalls.

Die Bewertungen der einzelnen Schwachstellen nach CVSS variieren. Während die WordPress-Community CVE-2026-60137 mit 5.3 von 10 nur einen mittleren Schweregrad attestiert, wird die Schwachstelle von anderen Stellen mit 9.1 als "kritisch" eingeschätzt [NVD26b]. Die Abweichungen ergeben sich nach CVSS in Version 3.x insbesondere aus unterschiedlichen Bewertungen der Angriffskomplexität und den zu erwartenden Auswirkungen auf die Schutzziele. Letztere werden auch für CVE-2026-63030 unterschiedlich eingeschätzt, sodass die Scores zwischen 7.5 (hoch) und 9.8 (kritisch) variieren [NVD26a].

In Kombination betrachtet kann die Schwachstellenkette "wp2shell" jedoch mit einem CVSS3.1-Score von 9.8 bewertet werden.

Das Unternehmen Searchlight Cyber hat weitere Details zu "wp2shell" veröffentlicht und wie sie auf die Schwachstellenkette gekommen sind. Demnach wurde die Schwachstelle mit Hilfe von OpenAI-5.6 Sol Ultra gefunden. Weitere technische Details zu "wp2shell" sowie den KI-Prompts finden sich im Blog des Unternehmens [SC26c].

Betroffene Produkte

Betroffen vom oben genannten Sachverhalt sind folgende Versionen:

- WordPress 6.8.x < 6.8.6 (nur von CVE-2026-60137 betroffen)
- WordPress 6.9.x < 6.9.5
- WordPress 7.0.x < 7.0.2
- WordPress 7.1 beta < 7.1 beta2

NICHT betroffen von einer der beiden Schwachstellen sind Versionen älter als WordPress 6.8.

Bewertung

WordPress ist eine weit verbreitetes Content Management System (CMS), welches bei Bloggern, Webshops und Webseiten-Betreibern sehr beliebt ist.

Die Schwachstellen sind aufgrund der Existenz von Proof-of-Concepts (PoCs) und der Einfachheit der Ausnutzung als sehr kritisch einzuschätzen, sofern keine automatisierten Updates genutzt werden. Die Ausnutzung der Schwachstellen erfordert keinerlei Authentifizierung. Ein Proof-of-Concept ist mittlerweile öffentlich und es ist davon auszugehen, dass Angreifer bereits begonnen haben den Code zu analysieren.

Es besteht eine hohe Wahrscheinlichkeit, dass zeitnah Angriffe auf WordPress-Instanzen durchgeführt werden.

Update 1:

Nur wenige Stunden nach der Veröffentlichung wurden erste Proof-of-Concepts im Internet verbreitet. Kurz darauf gab es auch Berichte über die ersten Ausnutzungen. Der Sachverhalt "wp2shell" veranschaulicht erneut die gesunkene Zeit bis zur Ausnutzung von Schwachstellen ("Time-to-Exploit").

WordPress-Betreiber, die automatische Updates deaktiviert haben oder in Nutzungsszenarien, in denen die automatischen Updates aufgrund von Problemen mit bspw. den Dateiberechtigungen nicht funktionieren, sollten schnellstmöglich die abgesicherten Versionen manuell installieren. Alle Betreiber sollten sicherstellen, dass ihre Webseiten mit abgesicherten Versionen betrieben werden.

Aufgrund der öffentlichen PoCs sowie der bekannten Ausnutzung sollten Betreiber, deren Webseiten nicht automatisch am Tag der Veröffentlichung aktualisiert wurden, diese zudem auf eine bereits stattgefundene Kompromittierung prüfen.

Der Sachverhalt "wp2shell" betrifft gegenüber anderen mit WordPress verbundenen Schwachstellenausnutzungen das CMS in seiner Standardinstallation selbst und keine einzelnen Plugins oder Themes, die nur auf einzelnen Webseiten installiert wurden.

Auch wenn in Deutschland mehrere Millionen Webseiten mit WordPress betrieben werden, verringern der eingeschränkte betroffene Versionsbereich, der Einsatz von Web Application Firewalls (WAF) sowie die standardmäßig aktivierten automatischen Updates die Wahrscheinlichkeit einer sehr breiten Angriffswelle. Dennoch können verwundbare WordPress Seiten kurz- und mittelfristig zum Ziel von automatisierten Angriffen werden, die bspw. Cryptominer, Backdoors oder Ransomware installieren, oder auch von gezielten Angriffen, die die Schwachstellen bspw. nutzen, um Webseiteninhalte zu manipulieren oder (ggf. Kunden) Daten abzugreifen.

Maßnahmen

Mitigation

IT-Sicherheitsverantwortliche und Betreiber sollten schnellstmöglich sicherstellen, dass eine der abgesicherten Versionen automatisch installiert wurde oder diese ggf. manuell installieren.

Die Versionen 6.9.5, 7.0.2 und 7.1 beta2 schließen beide Schwachstellen.
Die Version 6.8.6 schließt die Schwachstelle CVE-2026-60137, durch CVE-2026-63030 besteht keine Betroffenheit für 6.8.x.

Betreiber können mit dem von Searchlight Cyber bereitgestellten Webseiten-Checker [SC26b] prüfen, ob eine Betroffenheit ihrer Webseiten besteht.

Workarounds

Neben den Patches wurden folgende Workarounds zur temporären Schließung der Schwachstellen empfohlen:

- Blockieren von Aufrufen zu "*/wp-json/batch/v1*" sowie mit dem Parameter "*?rest_route=/batch/v1*" mit Hilfe einer Web Application Firewall (WAF)
- Die Installation eines Plugins zur Blockierung von Anonymous-Anmeldungen an der REST-API der WordPress-Instanz - siehe [SC26b].

Kompromittierung prüfen

Update 1:

Aktuell verfügbare Berichte empfehlen die Prüfung folgender Parameter [LINK26], [EYE26]:

- Suche nach POST Requests im Zusammenhang mit /wp-json/batch/v1, insbesondere eine erhöhte Menge an Anfragen ist verdächtig
- Suche nach Requests mit ?rest_route=/batch/v1,
- Login-Versuche mit wp2_* , w2s_*,
- Admin-Konten in Verbindung mit den Mailadressen @wp2shell.invalid , @wp2shell.shellcode.lol
- Änderungen und Auffälligkeiten in oembed_cache und customize_changeset
- Weitere neue oder angepasste Dateien, Plugins und Konten insbesondere neue Administratoren-Konten
- Die Ausführung ungewöhnlicher Prozesse/Shell-Befehle auf dem Webserver
- Ungewöhnliche ausgehende Verbindungen

Im Falle eines Verdachts auf eine Ausnutzung der Schwachstellen sollten alle Passwörter der Nutzerkonten zurückgesetzt werden, da mit Hilfe der SQL-Injektion Schwachstelle (CVE-2026-60137) alle Passwort-Hashes der *wp_users* Tabelle ausgelesen und diese dann offline geknackt werden können.

Weiterhin sollte das betroffene System isoliert und mit der Beweissicherung begonnen werden. Ebenfalls sollten aktive Session beendet und – sofern möglich – auch das Neu-Aufsetzen des Systems in Betracht gezogen werden.

Mit der WordPress-Instanz in Verbindung stehende IT-Systeme sollten ebenfalls auf eine Kompromittierung geprüft werden [LINK26].

Empfehlungen

Update 1:

Das BSI empfiehlt Webseitenbetreiber zu prüfen, ob automatische Updates aktiviert und auch installiert werden können, sofern dies gewünscht ist. Sollten automatische Updates deaktiviert sein, so sollte das Aufkommen neuer Sicherheitsupdates beobachtet und Maßnahmen getroffen werden, die ein kurzfristiges installieren dieser erlaubt.

Betreiber von Webseiten mit wichtigen Dienstleistungen sollten grundsätzlich erwägen, eine Web Application Firewall (WAF) einzusetzen, um Angriffe kurzfristig und vorübergehend auch anderweitig abwehren zu können.

Referenzen

[WP26] WordPress 7.0.2 Release
https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

[NVD26a] CVE-2026-63030
https://nvd.nist.gov/vuln/detail/CVE-2026-63030

[NVD26b] CVE-2026-60137
https://nvd.nist.gov/vuln/detail/CVE-2026-60137

[Rapid7] CVE-2026-63030: wp2shell a Critical Remote Code Execution Vulnerability in WordPress Core,
https://www.rapid7.com/blog/post/etr-cve-2026-63030-wp2shell-a-critical-remote-code-execution-vulnerability-in-wordpress-core/

[SC26a] Searchlight Cyber wp2shell: Pre Authentication RCE in WordPress Core
https://slcyber.io/research-center/wp2shell-pre-authentication-rce-in-wordpress-core

[SC26b] Searchlight Cyber wp2shell: Pre Authentication RCE in WordPress Core
https://wp2shell.com/

Update 1:

[SC26c] Searchlight Cyber wp2shell: Exploit brokers pay 500000 for a WordPress-RCE I found one with GPT-5.6
https://slcyber.io/research-center/exploit-brokers-pay-500000-for-a-wordpress-rce-i-found-one-with-gpt5-6/

[EYE26] wp2shell: a defender's guide (CVE-2026-63030 + CVE-2026-60137):
https://research.eye.security/wp2shell-defenders-guide/

[LINK26] LinkedIn: Beitrag von Maurice Fielenbach:
https://www.linkedin.com/posts/mauricefielenbach_threatintel-wordpress-cybersecurity-share-7484215399744614401-3KpG/

Versionsverlauf

Version 1.0 — 18.07.2026
Version 1.1 — 20.07.2026

Mit den hier veröffentlichten Informationen weist das BSI anlassbezogen auf Sicherheitsrisiken mit herausragendem Bedrohungspotenzial hin. Bitte beachten Sie außerdem die tagesaktuellen Hinweise im WID-Portal auf https://www.cert-bund.de, um IT-Komponenten vor Cyber-Angriffen zu schützen.

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.