



Wiceprezes Rady Ministrów Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.57.2026
Warszawa, 04 sierpnia 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa¹

nr 2026/33/4

dotycząca podatności w oprogramowaniu WordPress

Rekomenduję podmiotom krajowego systemu cyberbezpieczeństwa² niezwłoczne zaktualizowanie wszystkich instancji WordPress do wersji:

- 7.1 beta2,
- 7.0.2,
- 6.9.5 lub 6.8.6 w zależności od aktualnie używanej gałęzi,

przeprowadzenie audytu logów systemu pod kątem nietypowych zapytań do REST API oraz parametrów WP_Query, zablokowanie dostępu do całego REST API np. za pomocą pluginu, lub zablokowanie dostępu do ścieżki `/wp-json/batch/v1` oraz parametr `?rest_route=/batch/v1` na poziomie rozwiązania typu WAF.

Podatność CVE-2026-63030 typu Interpretation Conflict dotyczy usługi REST API w systemie WordPress i w połączeniu z podatnością CVE-2026-60137, pozwala na przeprowadzenie ataku SQL Injection z możliwością zdalnego wykonania kodu (RCE).

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa przeprowadził konsultację w powyższym zakresie z CSIRT NASK, CSIRT GOV oraz CSIRT MON, na podstawie której została potwierdzona możliwość wystąpienia incydentu krytycznego w przypadku niezastosowania się do powyższej rekomendacji. Tym samym stwierdza się, że stosowanie oprogramowania z ww. podatnościami ma negatywny wpływ na bezpieczeństwo publiczne i istotny interes bezpieczeństwa państwa.

Podmiot krajowego systemu cyberbezpieczeństwa może wnieść zastrzeżenia do niniejszej rekomendacji na zasadach określonych w ustawie o KSC³.

Krzysztof Gawkowski

Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
/dokument podpisany elektronicznie/

¹ Rekomendacja wydana na podstawie art. 33 ust. 4a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, z późn. zm.), zwanej dalej „ustawą o KSC”.

² Podmioty, o których mowa w art. 4 ustawy o KSC.

³ Art. 33 ust. 5 ustawy o KSC.