Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0250

Kwetsbaarheden verholpen in WordPress door Automattic

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 18-07-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Er zijn twee kwetsbaarheden verholpen in WordPress Core 6.8.6, 6.9.5 en 7.0.2

Duiding

Een ongeauthenticeerde kwaadwillende kan de kwetsbaarheden op afstand misbruiken voor het uitvoeren van willekeurige code. Hiertoe dient een malafide HTTP-request naar de batch-API van een WordPress-site te worden verstuurd.

Aangezien kwetsbaarheden in contentmanagementsystemen structureel de interesse van kwaadwillenden hebben, verwacht het NCSC dat de kwetsbaarheden op korte termijn zullen gaan worden misbruikt.

Oplossingen

WordPress heeft beveiligingsupdates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Het NCSC adviseert om deze updates op korte termijn te installeren. Indien het installeren van de beveiligingsupdates niet mogelijk is, kan misbruik worden voorkomen door de mitigerende maatregelen toe te passen die door beveiligingsbedrijf Searchlight Cyber zijn gedeeld. Zie de bijgevoegde referenties voor meer informatie.

Referenties

- https://slcyber.io/research-center/wp2shell-pre-authentication-rce-in-wordpress-core
- https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-60137	5.9 MEDIUM
CVE-2026-63030	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CWE-436	Interpretation Conflict

Getroffen producten

WordPress
WordPress

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.