Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0389

Kwetsbaarheid verholpen in WordPress

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-09-2026
Revisie: 1.0.1

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

Update Revisie 1

Openbare bronnen melden dat er misbruik van de kwetsbaarheid is waargenomen. De kwetsbaarheid heeft echter wel een aantal randvoorwaarden nodig voor misbruik. De kwetsbaarheid is sterk afhankelijk van individuele configuratie.

Feiten

De ontwikkelaars van WordPress hebben een kwetsbaarheid verholpen in WordPress.

Duiding

Een kwaadwillende kan de kwetsbaarheid met kenmerk CVE-2026-87902 misbruiken, om zonder authenticatie een lokaal PHP-bestand buiten de actieve themamappen door WordPress te laten inladen. Onder bepaalde voorwaarden met betrekking tot het actieve thema en de serverconfiguratie kan de kwetsbaarheid leiden tot het uitvoeren van willekeurige code op de server. Hierdoor kan een kwaadwillende mogelijk toegang krijgen tot gevoelige gegevens, wijzigingen aanbrengen of verdere controle verkrijgen over de getroffen WordPress-installatie.

**Update: **Openbare bronnen melden dat er misbruik van de kwetsbaarheid is waargenomen.

Oplossingen

De kwetsbaarheid is verholpen in WordPress 7.1.2 en de beveiligingsupdate is ook beschikbaar gesteld voor ondersteunde oudere versies. Gebruikers wordt aangeraden zo spoedig mogelijk te upgraden naar een gepatchte versie. Zie de bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5whp

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-87902	9.2 CRITICAL

CWE's

CWE	Beschrijving
CWE-98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

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.