Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0466

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in WordPress Core

Publicatiedatum: 04-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

WordPress heeft een kwetsbaarheid verholpen in WordPress Core versies 4.7 tot en met 7.1.3.

Duiding

De kwetsbaarheid maakt misbruik mogelijk van een TOCTOU-racecondition (Time-of-Check to Time-of-Use) tijdens volledige WordPress Core-upgrades. Hierdoor kan een niet-geauthenticeerde aanvaller op afstand code uitvoeren op de server door het korte upgradevenster te misbruiken waarin de stagingdirectories via het web toegankelijk zijn.

Voor succesvolle exploitatie moet de aanvaller erin slagen om tijdens dit beperkte upgradevenster de racecondition te benutten.

CISA heeft bevestigd dat CVE-2026-119977 actief wordt misbruikt en heeft de kwetsbaarheid op 3 november 2026 toegevoegd aan de Known Exploited Vulnerabilities (KEV)-catalogus.

Oplossingen

WordPress heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://wordpress.org/news/2026/10/wordpress-7-1-4/
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordpress-core-470-713-unauthenticated-upgrade-window-staged-installer-remote-code-execution?asset_slug=wordpress

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-119977	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code
CWE-552	Files or Directories Accessible to External Parties
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition

Getroffen producten

WordPress
WordPress Core

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.