Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0524

PRIORITEIT: HOOG

Kwetsbaarheid verholpen in Drupal core

Publicatiedatum: 26-11-2026

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 delen. 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

Drupal heeft een nieuwe kwetsbaarheid verholpen in Drupal core, specifiek in het install.php bestand en in versies tot 10.6.23 en van 11.0.0 tot 11.4.14.

Duiding

Het install.php bestand bevatte kwetsbaarheden die konden leiden tot overname van de site indien het bestand toegankelijk bleef na de SA-CORE-2026-017 advisory, warvoor het NCSC de eerdere advisory NCSC-2026-0507 heeft gepubliceerd.

Daarnaast is er een Improper Check for Unusual or Exceptional Conditions kwetsbaarheid aanwezig in de genoemde versies, die Forceful Browsing aanvallen mogelijk maakt. Deze kwetsbaarheden betreffen authenticatieomzeiling en ongeautoriseerde toegang binnen Drupal core.

Drupal maakt melding van misbruik van deze nieuwe kwetsbaarheid, ook in systemen die weliswaar gepatched zijn naar het niveau van SA-CORE-2026-017, maar door het niet volledig uitvoeren van de geadviseerde systeem-hardening kwetsbaar bleven.

Oplossingen

Drupal heeft updates uitgebracht om deze kwetsbaarheid te verhelpen. Tevens adviseert Drupal om extra maatregelen te nemen om de installer beter te beveiligen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://advisories.ncsc.nl/2026/ncsc-2026-0507.html
- https://www.drupal.org/docs/administering-a-drupal-site/security-in-drupal/securing-the-installer-installphp
- https://www.drupal.org/sa-core-2026-017
- https://www.drupal.org/sa-core-2026-019

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-136716	

CWE's

CWE	Beschrijving
CWE-754	Improper Check for Unusual or Exceptional Conditions

Getroffen producten

Drupal
Drupal 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.