Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0507

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Drupal core

Publicatiedatum: 18-11-2026

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

Drupal heeft kwetsbaarheden verholpen in Drupal core.

Duiding

De eerste kwetsbaarheid betreft een potentiële gadget chain gerelateerd aan onveilige deserialisatie binnen Drupal core. Deze kwetsbaarheid is op zichzelf niet direct exploiteerbaar, maar kan worden misbruikt in combinatie met een andere fout die het mogelijk maakt onveilige input te deserialiseren, wat kan leiden tot remote code execution. De tweede kwetsbaarheid betreft het install.php-script van Drupal core, dat onder specifieke omstandigheden kan worden misbruikt om een site opnieuw te installeren. Dit gebeurt wanneer de installer niet correct is beveiligd of verwijderd na de initiële installatie, waardoor een aanvaller arbitrary code kan uitvoeren of de controle over de site kan overnemen door authenticatie- en configuratiecontroles te omzeilen.

Oplossingen

Drupal heeft updates uitgebracht om deze kwetsbaarheden in Drupal core te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.drupal.org/sa-core-2026-017
- https://www.drupal.org/sa-core-2026-018
- https://www.drupal.org/security

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-132166	
CVE-2026-132165	

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Functionality
CWE-502	Deserialization of Untrusted Data

Getroffen producten

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.