



Advisory NCSC-2026-0438

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Drupal Core en modules door Drupal

Publicatiedatum: 19-10-2026

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 kwetsbaarheden verholpen in de Drupal core Field UI module, Entity List module, Navigation module, Link module en het Gin administratie thema.

Duiding

De kwetsbaarheden betreffen meerdere modules binnen Drupal. In de Field UI module en de Entity List module is een remote code execution kwetsbaarheid aanwezig die kan worden misbruikt via contributed modules of custom code, waarbij sommige aanvalspaden geen authenticatie vereisen. De Navigation module, Link module en het Gin administratie thema bevatten cross-site scripting (XSS) kwetsbaarheden veroorzaakt door onvoldoende sanitatie van bepaalde HTML- of URL-attributen. De XSS-kwetsbaarheden kunnen alleen worden misbruikt door gebruikers met specifieke permissies, zoals het invoeren van HTML met bepaalde data-attributen of de 'administer menu' permissie. De kwetsbaarheden zijn specifiek voor Drupal installaties die deze modules of thema's gebruiken en kunnen leiden tot ongeautoriseerde code-uitvoering of scriptinjectie.

De kwetsbaarheden zijn niet zondermeer te misbruiken, maar vereisen een plugin of externe module waarmee de kwetsbaarheid kan worden misbruikt. Het is daarom aan te raden om geen gebruik te maken van onbekende, en onvertrouwde, plugins en externe modules.

Oplossingen

Drupal heeft updates uitgebracht om de kwetsbaarheden in de genoemde modules en het Gin thema te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.drupal.org/sa-contrib-2026-218>
- <https://www.drupal.org/sa-contrib-2026-219>
- <https://www.drupal.org/sa-core-2026-014>
- <https://www.drupal.org/sa-core-2026-015>
- <https://www.drupal.org/sa-core-2026-016>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-108097	
CVE-2026-108099	
CVE-2026-108514	
CVE-2026-108515	
CVE-2026-110738	

CWE's

CWE	Beschrijving
CWE-732	Incorrect Permission Assignment for Critical Resource

Getroffen producten

Drupal
core

drupal
entity_list
gin

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 or 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.