Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0474

Kwetsbaarheden verholpen in Drupal Core

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-12-2024

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

Feiten

Drupal heeft kwetsbaarheden verholpen in Drupal Core (Specifiek voor versies 7.0 tot 7.102, 8.0.0 tot voor 10.2.11, 10.3.0 tot voor 10.3.9, en 11.0.0 tot voor 11.0.8).

Duiding

De kwetsbaarheden in Drupal Core zijn gerelateerd aan privilege-escalatie en de deserialisatie van niet-vertrouwde gegevens, wat kan leiden tot objectinjectie. Deze kwetsbaarheden kunnen worden misbruikt door ongeautoriseerde gebruikers om verhoogde privileges te verkrijgen of om de applicatiegedraging te manipuleren, wat kan resulteren in ongeautoriseerde toegang tot gevoelige gegevens.

Oplossingen

Drupal heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.drupal.org/sa-core-2024-003
- https://www.drupal.org/sa-core-2024-004
- https://www.drupal.org/sa-core-2024-005
- https://www.drupal.org/sa-core-2024-006
- https://www.drupal.org/sa-core-2024-007
- https://www.drupal.org/sa-core-2024-008

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-12393	
CVE-2024-55634	
CVE-2024-55635	
CVE-2024-55636	
CVE-2024-55637	

- CVE-2024-55638

CWE's

CWE	Beschrijving
CWE-289	Authentication Bypass by Alternate Name
CWE-178	Improper Handling of Case Sensitivity
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

drupal
drupal
open_source
drupal

Disclaimer