Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0018

Kwetsbaarheden verholpen in TYPO3 CMS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-01-2026

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

TYPO3 heeft kwetsbaarheden verholpen in TYPO3 CMS (Specifiek voor bepaalde versies).

Duiding

De kwetsbaarheden in TYPO3 CMS stellen aanvallers in staat om veldniveau-toegangscontroles te omzeilen, ongeautoriseerde gegevens in te voegen in beperkte databasevelden, en om redirectrecords te manipuleren zonder enige restricties. Daarnaast kunnen backend-gebruikers met toegang tot de recycler-module gegevens verwijderen uit elke database tabel zonder de noodzakelijke machtigingen. Ook kunnen lokale gebruikers met schrijftoegang tot de mail-file spool directory willekeurige PHP-code uitvoeren via onveilige deserialisatie. Deze kwetsbaarheden kunnen leiden tot ernstige risico's voor de integriteit van gegevens en de beschikbaarheid van de site.

Oplossingen

TYPO3 heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://typo3.org/security/advisory/typo3-core-sa-2026-001
- https://typo3.org/security/advisory/typo3-core-sa-2026-002
- https://typo3.org/security/advisory/typo3-core-sa-2026-003
- https://typo3.org/security/advisory/typo3-core-sa-2026-004

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-59020	5.3 MEDIUM
CVE-2025-59021	5.3 MEDIUM
CVE-2025-59022	7.1 HIGH
CVE-2026-0859	5.2 MEDIUM

CWE's

CWE	Beschrijving
CWE-502	Deserialization of Untrusted Data
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization

Getroffen producten

TYPO3
CMS
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.