Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0516

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Joomla! Core door Joomla

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 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

Joomla heeft meerdere kwetsbaarheden verholpen in Joomla! Core, inclusief componenten zoals com_newsfeeds, com_contact, com_media, com_menus, com_workflow, com_fields, com_scheduler, com_finder, com_associations, com_banners, com_modules, com_installer, com_guidedtours, mod_articles_popular, en de webservice endpoints, verspreid over versies 1.5.0 tot en met 6.2.0.

Duiding

De kwetsbaarheden betreffen onder andere improper Access Control List (ACL) checks die leiden tot het omzeilen van permissiebeperkingen, waardoor ongeautoriseerde gebruikers toegang kunnen krijgen tot beschermde content, menu-items, contactgegevens, nieuwsfeeds, media bestanden en workflow stages.

Er zijn meerdere cross-site scripting (XSS) kwetsbaarheden, zowel reflected als stored, die het mogelijk maken om kwaadaardige scripts te injecteren en uit te voeren binnen verschillende componenten en modules van Joomla!. Daarnaast zijn er kwetsbaarheden die leiden tot informatielekken, zoals het blootstellen van gevoelige configuratiegegevens, SMTP OAuth2 tokens en schema data op foutpagina's. Verder zijn er kwetsbaarheden die Denial-of-Service (DoS) kunnen veroorzaken door inefficiënte verwerking van invoer, zoals in de smart search query parser en email cloaking plugin.

Ook is er een remote code execution (RCE) kwetsbaarheid door onvoldoende escaping van media custom field parameters. Path traversal kwetsbaarheden maken het mogelijk om bestanden buiten de bedoelde directories te lezen of te wijzigen. Tenslotte zijn er problemen met sessiebeheer, zoals het niet ongeldig maken van wachtwoord reset tokens en het mogelijk beëindigen van sessies van andere gebruikers zonder toestemming.

Deze kwetsbaarheden zijn aanwezig in meerdere grote versies van Joomla! Core en gerelateerde componenten.

Oplossingen

Joomla heeft updates uitgebracht om de kwetsbaarheden te verhelpen in de genoemde versies van Joomla! Core en de betrokken componenten. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://developer.joomla.org/security-centre/1099-20261101-core-improper-acl-checks-in-webservice-endpoints.html
- https://developer.joomla.org/security-centre/1100-20261102-core-improper-acl-checks-in-com-newsfeeds-delete-action.html
- https://developer.joomla.org/security-centre/1101-20261103-core-information-disclosure-in-schema-org-system-plugin.html
- https://developer.joomla.org/security-centre/1102-20261104-core-xss-in-com-finder-search-view.html
- https://developer.joomla.org/security-centre/1103-20261105-core-information-disclosure-in-com-contact-associations.html
- https://developer.joomla.org/security-centre/1104-20261106-core-improper-access-checks-in-com-contact-category-view.html
- https://developer.joomla.org/security-centre/1105-20261107-core-insufficient-file-extension-checks-in-com-media-rename-and-copy-actions.html
- https://developer.joomla.org/security-centre/1106-20261108-core-improper-access-checks-in-com-contact-form-submission.html
- https://developer.joomla.org/security-centre/1107-20261109-core-information-disclosure-in-com-content-tag-filter.html
- https://developer.joomla.org/security-centre/1108-20261110-core-information-disclosure-in-mod-articles-popular.html
- https://developer.joomla.org/security-centre/1109-20261111-core-missing-authentication-in-web-installer.html
- https://developer.joomla.org/security-centre/1110-20261112-core-local-file-inclusion-through-language-parameter.html
- https://developer.joomla.org/security-centre/1111-20261113-core-improper-acl-checks-in-com-media-file-overwrite.html
- https://developer.joomla.org/security-centre/1112-20261114-core-improper-acl-checks-in-com-menus-webservice-endpoint.html
- https://developer.joomla.org/security-centre/1113-20261115-core-improper-acl-checks-for-target-categories-in-webservice-endpoints.html
- https://developer.joomla.org/security-centre/1114-20261116-core-information-disclosure-in-com-config-webservice-endpoint.html
- https://developer.joomla.org/security-centre/1115-20261117-core-race-condition-in-formatted-text-logger.html
- https://developer.joomla.org/security-centre/1116-20261118-core-xss-in-com-contact-name.html
- https://developer.joomla.org/security-centre/1117-20261119-core-xss-in-com-newsfeeds-name.html
- https://developer.joomla.org/security-centre/1118-20261120-core-xss-in-com-guidedtours-tour-and-step-titles.html

- https://developer.joomla.org/security-centre/1119-20261121-core-xss-in-com-contenthistory-version-preview.html
- https://developer.joomla.org/security-centre/1120-20261122-core-xss-in-com-associations-association-view.html
- https://developer.joomla.org/security-centre/1121-20261123-core-xss-in-com-associations-modal.html
- https://developer.joomla.org/security-centre/1122-20261124-core-xss-in-form-field-showon-attribute.html
- https://developer.joomla.org/security-centre/1123-20261125-core-xss-in-note-custom-field.html
- https://developer.joomla.org/security-centre/1124-20261126-core-xss-in-administrator-menu-module.html
- https://developer.joomla.org/security-centre/1125-20261127-core-xss-in-com-modules-module-positions.html
- https://developer.joomla.org/security-centre/1126-20261128-core-xss-in-com-installer-language-installation-view.html
- https://developer.joomla.org/security-centre/1127-20261129-core-xss-in-module-titles.html
- https://developer.joomla.org/security-centre/1128-20261130-core-xss-in-com-scheduler-task-title.html
- https://developer.joomla.org/security-centre/1129-20261131-core-xss-in-com-banners-banner-name.html
- https://developer.joomla.org/security-centre/1130-20261132-core-dos-in-com-finder-search-query.html
- https://developer.joomla.org/security-centre/1131-20261133-core-missing-authentication-in-com-privacy-request-form.html
- https://developer.joomla.org/security-centre/1132-20261134-core-improper-root-user-check.html
- https://developer.joomla.org/security-centre/1133-20261135-core-improper-acl-checks-in-com-menus-site-modal.html
- https://developer.joomla.org/security-centre/1134-20261136-core-password-reset-token-not-invalidated-on-password-change.html
- https://developer.joomla.org/security-centre/1135-20261137-core-improper-access-checks-in-com-content-vote-task.html
- https://developer.joomla.org/security-centre/1136-20261138-core-dos-in-inputfilter-email-punycode-conversion.html
- https://developer.joomla.org/security-centre/1137-20261139-core-dos-in-email-cloaking-plugin.html
- https://developer.joomla.org/security-centre/1138-20261140-core-xss-in-joomla-dialog-header.html
- https://developer.joomla.org/security-centre/1139-20261141-core-xss-in-com-installer-changelog.html
- https://developer.joomla.org/security-centre/1140-20261142-core-improper-access-checks-in-com-login-logout-task.html
- https://developer.joomla.org/security-centre/1141-20261143-core-information-disclosure-in-get-request-task-plugin.html

- https://developer.joomla.org/security-centre/1142-20261144-core-csrf-token-leak-in-install-from-web.html
- https://developer.joomla.org/security-centre/1143-20261145-core-improper-acl-checks-in-com-media-file-creation.html
- https://developer.joomla.org/security-centre/1144-20261146-core-information-disclosure-in-global-configuration-smtp-oauth2-settings.html
- https://developer.joomla.org/security-centre/1145-20261147-core-information-disclosure-in-mail-template-smtp-oauth2-handling.html
- https://developer.joomla.org/security-centre/1146-20261148-core-information-disclosure-in-mail-template-smtp-settings.html
- https://developer.joomla.org/security-centre/1147-20261149-core-improper-acl-checks-in-com-contact-publishing-dates.html
- https://developer.joomla.org/security-centre/1148-20261150-core-improper-acl-checks-in-com-menus-publishing-dates.html
- https://developer.joomla.org/security-centre/1149-20261151-core-path-traversal-in-com-media-search.html
- https://developer.joomla.org/security-centre/1150-20261152-core-xss-in-module-title-attributes.html
- https://developer.joomla.org/security-centre/1151-20261153-core-improper-access-checks-for-category-view-levels-in-com-contact-and-com-newsfeeds.html
- https://developer.joomla.org/security-centre/1152-20261154-core-improper-acl-checks-in-com-workflow-stages.html
- https://developer.joomla.org/security-centre/1153-20261155-core-improper-acl-checks-in-com-fields.html
- https://developer.joomla.org/security-centre/1154-20261156-core-rce-through-media-custom-field-parameters.html
- https://developer.joomla.org/security-centre/1155-20261157-core-path-traversal-in-com-scheduler-task-log-file-name.html
- https://developer.joomla.org/security-centre/1156-20261158-core-dos-in-inputfilter-tag-cleaning.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-120653	6.9 MEDIUM
CVE-2026-120654	5.1 MEDIUM
CVE-2026-120655	6.3 MEDIUM
CVE-2026-120674	8.6 HIGH
CVE-2026-120675	6.3 MEDIUM
CVE-2026-123209	6.3 MEDIUM
CVE-2026-123210	8.9 HIGH
CVE-2026-123211	6.9 MEDIUM
CVE-2026-123212	6.3 MEDIUM
CVE-2026-123213	6.3 MEDIUM
CVE-2026-123214	9.2 CRITICAL
CVE-2026-126045	9.2 CRITICAL
CVE-2026-126046	5.5 MEDIUM
CVE-2026-127294	2.0 LOW
CVE-2026-127295	2.0 LOW
CVE-2026-127296	5.1 MEDIUM
CVE-2026-127297	9.2 CRITICAL
CVE-2026-127298	8.4 HIGH
CVE-2026-127299	8.4 HIGH
CVE-2026-127300	8.4 HIGH
CVE-2026-127301	8.4 HIGH
CVE-2026-127302	8.6 HIGH
CVE-2026-127303	8.6 HIGH
CVE-2026-127304	8.4 HIGH
CVE-2026-129362	8.4 HIGH
CVE-2026-129363	8.4 HIGH
CVE-2026-129364	8.4 HIGH
CVE-2026-129365	7.6 HIGH

CVE	CVSS Score
CVE-2026-129366	8.4 HIGH
CVE-2026-129367	8.4 HIGH
CVE-2026-129368	8.4 HIGH
CVE-2026-129369	6.9 MEDIUM
CVE-2026-129370	6.9 MEDIUM
CVE-2026-129371	7.7 HIGH
CVE-2026-129372	5.1 MEDIUM
CVE-2026-129373	6.3 MEDIUM
CVE-2026-129374	5.3 MEDIUM
CVE-2026-129375	5.1 MEDIUM
CVE-2026-129376	5.1 MEDIUM
CVE-2026-129377	7.6 HIGH
CVE-2026-129378	7.6 HIGH
CVE-2026-129379	6.9 MEDIUM
CVE-2026-129380	8.2 HIGH
CVE-2026-129381	7.4 HIGH
CVE-2026-129382	5.1 MEDIUM
CVE-2026-129383	6.3 MEDIUM
CVE-2026-129384	6.3 MEDIUM
CVE-2026-129385	6.3 MEDIUM
CVE-2026-129386	5.1 MEDIUM
CVE-2026-129387	5.1 MEDIUM
CVE-2026-129388	6.9 MEDIUM
CVE-2026-129389	8.4 HIGH
CVE-2026-129390	6.3 MEDIUM
CVE-2026-129391	5.1 MEDIUM
CVE-2026-129392	5.1 MEDIUM
CVE-2026-129393	9.4 CRITICAL
CVE-2026-129394	7.0 HIGH
CVE-2026-129395	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-91	XML Injection
CWE-98	Improper Control of Filename for Include/Require Statement in PHP Program
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-306	Missing Authentication for Critical Functionality
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-407	Inefficient Algorithmic Complexity
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-524	Use of Cache Containing Sensitive Information
CWE-552	Files or Directories Accessible to External Parties
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-640	Weak Password Recovery Mechanism for Forgotten Password
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-1024	Comparison of Incompatible Types

Getroffen producten

Joomla
Joomla!

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.