



NCSC-2026-0222

Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-07-2026

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

GitLab heeft meerdere kwetsbaarheden verholpen in GitLab Enterprise Edition (EE) en Community Edition (CE) in versies variërend van 9.1 tot voor 18.11.7, 19.0 tot voor 19.0.4, en 19.1 tot voor 19.1.2.

Duiding

De kwetsbaarheden betreffen onder andere:

- Het creëren van repositories met discrepanties tussen de webinterface en de daadwerkelijke downloadbare bestanden door onjuiste verwerking van Git reference names.
- Onvoldoende autorisatiecontroles in GraphQL-operaties waardoor gebruikers met auditor-permissies compliance violation records kunnen aanpassen.
- Cross-site scripting (XSS) waarbij gebruikers met developer-permissies kwaadaardige scripts kunnen injecteren in de browser van andere gebruikers door onjuiste inputsanitatie.
- Ongeautoriseerde detectie van private projecten door onbevoegde gebruikers via cross-project reference pages.
- Bypass van autorisatiecontroles waardoor gebruikers met minimale toegangsrechten metadata van werkitems in private projecten kunnen inzien.
- Toegang tot opgeslagen credentials van andere gebruikers door maintainers via onvoldoende toegangsbeperkingen.
- Ongeautoriseerde wijziging van groepsinstellingen door foutieve autorisatiecontroles op groepsniveau. Deze kwetsbaarheden maken het mogelijk voor gebruikers met verschillende toegangsrechten om acties uit te voeren of informatie in te zien die normaal gesproken beperkt zou moeten zijn, door het omzeilen van autorisatiecontroles of het misbruiken van onjuiste inputverwerking.

Oplossingen

GitLab heeft updates en patches uitgebracht voor de genoemde versies van de GitLab Editions om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-1-2-released/>

Kwetsbaarheden

CVE	CVSS Score

> CVE-2025-12506	3.5 LOW
> CVE-2026-6352	5.3 MEDIUM
> CVE-2026-6896	5.1 MEDIUM
> CVE-2026-7492	6.9 MEDIUM
> CVE-2026-8472	5.3 MEDIUM
> CVE-2026-11827	4.9 MEDIUM
> CVE-2026-13151	2.7 LOW
> CVE-2026-13320	7.3 HIGH

CWE's

CWE	Beschrijving
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CVE-522	Insufficiently Protected Credentials
> CVE-706	Use of Incorrectly-Resolved Name or Reference
> CVE-862	Missing Authorization
> CVE-863	Incorrect Authorization

Getroffen producten

GitLab
GitLab

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.