



# NCSC-2026-0103

## Kwetsbaarheden verholpen in GitLab

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 26-03-2026

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

GitLab heeft kwetsbaarheden verholpen in versies 18.8.7, 18.9.3, en 18.10.1.

## Duiding

De kwetsbaarheden omvatten onder andere denial-of-service scenario's die konden worden veroorzaakt door geauthenticeerde gebruikers via specifieke webhook configuraties en continue integratie inputs. Daarnaast waren er problemen met onjuiste toegangscontrole voor gebruikers met de Planner rol, waardoor gevoelige metadata toegankelijk was. Ongeauthenticeerde gebruikers konden API-tokens voor zelf-gehoste AI-modellen ophalen, en er waren ook kwetsbaarheden die het mogelijk maakten om WebAuthn twee-factor authenticatie te omzeilen. Verder waren er problemen met onvoldoende sanitization van Mermaid diagrammen en HTML-inhoud, wat leidde tot de mogelijkheid om ongeautoriseerde acties uit te voeren of gebruikersaccounts te manipuleren. Tot slot waren er tekortkomingen in CSRF-bescherming die ongeauthenticeerde gebruikers in staat stelden om GraphQL-mutaties uit te voeren.

## Oplossingen

GitLab heeft patches uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

➤ <https://about.gitlab.com/releases/2026/03/25/patch-release-gitlab-18-10-1-released/>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-13078</a>	6.5 MEDIUM
➤ <a href="#">CVE-2025-13436</a>	6.5 MEDIUM
➤ <a href="#">CVE-2025-14595</a>	4.3 MEDIUM
➤ <a href="#">CVE-2026-1724</a>	6.8 MEDIUM
➤ <a href="#">CVE-2026-2370</a>	
➤ <a href="#">CVE-2026-2726</a>	4.3 MEDIUM

> CVE-2026-2745	6.8 MEDIUM
> CVE-2026-2973	5.4 MEDIUM
> CVE-2026-2995	7.7 HIGH
> CVE-2026-3857	8.1 HIGH
> CVE-2026-3988	7.5 HIGH
> CVE-2026-4363	3.7 LOW

## CWE's

CWE	Beschrijving
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
> CWE-288	Authentication Bypass Using an Alternate Path or Channel
> CWE-306	Missing Authentication for Critical Function
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-407	Inefficient Algorithmic Complexity
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-862	Missing Authorization
> CWE-863	Incorrect Authorization
> CWE-1284	Improper Validation of Specified Quantity in Input

## Getroffen producten

<b>GitLab</b>
GitLab

**Open Source**

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.