



# NCSC-2025-0057

## Kwetsbaarheden verholpen in GitLab CE/EE

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-02-2025

**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 GitLab CE/EE (Specifiek voor versies 14.1 tot 17.8.2).

## Duiding

De kwetsbaarheden omvatten een denial-of-service kwetsbaarheid, een externe service interactie kwetsbaarheid, een kritieke XSS kwetsbaarheid, onjuiste autorisatie kwetsbaarheden, een onveilige directe objectreferentie kwetsbaarheid, een probleem met ingetrokken Personal Access Tokens, en een kritieke informatie openbaarmaking kwetsbaarheid. Deze kwetsbaarheden kunnen door kwaadwillenden worden misbruikt om de beschikbaarheid van de diensten te verstoren, ongeautoriseerde toegang te verkrijgen tot gevoelige gegevens, en gevoelige informatie te onthullen.

## Oplossingen

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

## Referenties

➤ <https://about.gitlab.com/releases/2025/02/12/patch-release-gitlab-17-8-2-released/>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2024-12379</a>	6.5 MEDIUM
➤ <a href="#">CVE-2024-3303</a>	
➤ <a href="#">CVE-2024-9870</a>	4.3 MEDIUM
➤ <a href="#">CVE-2025-0376</a>	8.7 HIGH
➤ <a href="#">CVE-2025-0516</a>	4.3 MEDIUM
➤ <a href="#">CVE-2025-1042</a>	4.9 MEDIUM
➤ <a href="#">CVE-2025-1198</a>	2.3 LOW
➤ <a href="#">CVE-2025-1212</a>	4.3 MEDIUM

## CWE's

CWE	Beschrijving
> <a href="#">CWE-441</a>	Unintended Proxy or Intermediary ('Confused Deputy')
> <a href="#">CWE-497</a>	Exposure of Sensitive System Information to an Unauthorized Control Sphere
> <a href="#">CWE-613</a>	Insufficient Session Expiration
> <a href="#">CWE-552</a>	Files or Directories Accessible to External Parties
> <a href="#">CWE-770</a>	Allocation of Resources Without Limits or Throttling
> <a href="#">CWE-863</a>	Incorrect Authorization
> <a href="#">CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>gitlab</b>
gitlab
<b>open_source</b>
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.