



NCSC-2025-0176

Kwetsbaarheden verholpen in GitLab

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-05-2025

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

GitLab heeft kwetsbaarheden verholpen in zowel de Community als Enterprise Editions van GitLab.

Duiding

De kwetsbaarheden omvatten onder andere het onterecht tonen van volledige e-mailadressen aan ongeautoriseerde gebruikers, onvoldoende invoervalidatie die kan leiden tot Denial-of-Service, en de mogelijkheid voor aanvallers om gemaskeerde CI-variabelen bloot te stellen. Daarnaast kunnen bepaalde gebruikers mogelijk de tweefactorauthenticatie omzeilen en kunnen geauthenticeerde gebruikers Denial-of-Service-aanvallen uitvoeren door serverresources uit te putten. Deze kwetsbaarheden hebben aanzienlijke gevolgen voor de privacy en beveiliging van gebruikersinformatie.

Oplossingen

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

Referenties

➤ <https://about.gitlab.com/releases/2025/05/21/patch-release-gitlab-18-0-1-released/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-7803	
➤ CVE-2025-0679	5.3 MEDIUM
➤ CVE-2024-9163	
➤ CVE-2025-3111	5.3 MEDIUM
➤ CVE-2025-4979	5.1 MEDIUM
➤ CVE-2025-0605	2.3 LOW
➤ CVE-2025-2853	5.3 MEDIUM
➤ CVE-2025-1110	5.1 MEDIUM

[> CVE-2024-12093](#)

2.3 LOW

[> CVE-2025-0993](#)

5.3 MEDIUM

CWE's

CWE	Beschrijving
> CVE-1288	Improper Validation of Consistency within Input
> CVE-359	Exposure of Private Personal Information to an Unauthorized Actor
> CVE-1390	Weak Authentication
> CVE-1220	Insufficient Granularity of Access Control
> CVE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

GitLab

Community Edition,
Enterprise Edition

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.