Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0161

Kwetsbaarheden verholpen in GitLab door GitLab Inc.

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-05-2026

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 Inc. heeft meerdere kwetsbaarheden verholpen in GitLab Community Edition (CE) en Enterprise Edition (EE) in diverse versies, met name in releases van versie 8.3 tot en met 18.11.3.

Duiding

De kwetsbaarheden betreffen verschillende componenten en functionaliteiten binnen GitLab, waaronder de Jira-integratie, container registry, virtual registry upstreams, merge request approval policies, debugging symbol downloads, analytics dashboards, package management, issue tracking, project- en groepslidmaatschapsbeheer, en API inputvalidatie.

Aanvallers kunnen onder meer:

- Authenticeerde gebruikers kunnen Jira-issues buiten hun projecttoegang bekijken door onvoldoende toegangscontrole.
- Ongeauthenticeerde gebruikers kunnen zonder CSRF-bescherming ongeautoriseerde Jira-subscripties aanmaken.
- Ongeauthenticeerde gebruikers kunnen door onvoldoende inputvalidatie een denial-of-service veroorzaken via speciaal opgemaakte verzoeken of uploads.
- Authenticeerde gebruikers met ontwikkelaarsrechten kunnen beschermde container registry tags verwijderen en package protection regels omzeilen.
- Authenticeerde gebruikers kunnen merge request goedkeuringsvereisten omzeilen door het verwijderen van approval rules.
- Ongeautoriseerde toegang tot interne hosts is mogelijk via virtual registry upstreams door onvoldoende validatie.
- Cross-site scripting (XSS) aanvallen zijn mogelijk door onvoldoende inputsanitatie in analytics dashboards, e-mail notificaties en andere gebruikersinvoervelden.
- OAuth tokens met read_api scope kunnen misbruikt worden om issues in private projecten aan te maken en te becommentariëren.
- Authenticeerde gebruikers met Guest-permissies kunnen toegang krijgen tot projectissues die beperkt zouden moeten zijn.
- Ongeautoriseerde gebruikers kunnen private groepslidmaatschappen enumereren.

Deze kwetsbaarheden zijn aanwezig in meerdere opeenvolgende versies van GitLab CE en EE, wat wijst op terugkerende problemen in toegangscontrole, inputvalidatie en autorisatie binnen het platform.

Oplossingen

GitLab Inc. heeft updates en patches uitgebracht voor de genoemde versies om de diverse kwetsbaarheden te verhelpen. Gebruikers wordt geadviseerd de meest recente updates te installeren om de beveiliging van hun GitLab-omgevingen te waarborgen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-18-11-3-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-3160	6.9 MEDIUM
CVE-2026-4527	5.3 MEDIUM
CVE-2026-1659	6.9 MEDIUM
CVE-2026-1338	5.3 MEDIUM
CVE-2026-7471	2.3 LOW
CVE-2026-6883	2.1 LOW
CVE-2026-3074	5.3 MEDIUM
CVE-2026-7377	5.1 MEDIUM
CVE-2026-8280	5.3 MEDIUM
CVE-2026-4524	6.9 MEDIUM
CVE-2026-8144	5.3 MEDIUM
CVE-2026-1184	5.3 MEDIUM
CVE-2026-1322	2.3 LOW
CVE-2026-7481	5.1 MEDIUM
CVE-2026-6335	5.1 MEDIUM

CVE-2026-3073	**5.3 MEDIUM**
CVE-2025-12669	**5.1 MEDIUM**
CVE-2026-6073	**5.1 MEDIUM**
CVE-2026-2900	**5.1 MEDIUM**
CVE-2026-6063	**5.3 MEDIUM**
CVE-2025-13874	**5.3 MEDIUM**
CVE-2026-3607	**5.3 MEDIUM**
CVE-2025-14870	**6.9 MEDIUM**
CVE-2025-14869	**6.9 MEDIUM**
CVE-2026-5297	

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')
CWE-502	Deserialization of Untrusted Data
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-840	Business Logic Errors
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery (SSRF)

CWE-1280	Access Control Check Implemented After Asset is Accessed
CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

GitLab
Community Edition, Enterprise Edition

Disclaimer