Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0211

Kwetsbaarheden verholpen in GitLab Community Edition en Enterprise Edition

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 25-06-2026

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 Enterprise Edition (EE) en andere GitLab versies, specifiek in releases van versie 8.3 tot en met 19.1.1, met nadruk op versies rond 18.11.6, 19.0.3 en 19.1.1.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van GitLab, waaronder de package management system, DAST site profile management, CI/CD API endpoints, Snippet feature, mirror synchronisatie, en project issue tracking. Diverse problemen zijn gerelateerd aan onjuiste autorisatiecontroles, onvoldoende validatie van input en output, en onjuiste filtering van gevoelige data. Hierdoor kunnen gebruikers met beperkte of geauthenticeerde rechten onder andere:

- toegang krijgen tot metadata van pakketten ondanks uitgeschakelde registraties,
- beveiligingsregels voor pakketten omzeilen en metadata overschrijven,
- geheimen uit DAST site profielen uitlezen,
- cross-site scripting (XSS) aanvallen uitvoeren via onvoldoende padvalidatie en input sanitatie,
- beschermde omgevingsconfiguraties benaderen of wijzigen ondanks zichtbaarheid-instellingen,
- verborgen of ongeautoriseerde inhoud in Snippets plaatsen,
- gevoelige projectinformatie inzien zonder juiste rechten,
- client-side code injecteren in sessies van andere gebruikers,
- gevoelige informatie in logs laten verschijnen door onvoldoende filtering,
- vertrouwelijke issue-referenties op publieke projecten benaderen zonder authenticatie,
- interne netwerkresources benaderen via mirror synchronisatie door onvoldoende URL-validatie,
- en virtuele registry cleanup policies van andere groepen aanpassen door onvoldoende toegangscontrole.

Deze kwetsbaarheden zijn aanwezig in meerdere opeenvolgende versies van GitLab en betreffen zowel authenticatie- als autorisatieproblemen, alsmede input- en outputvalidatie.

Oplossingen

GitLab heeft updates en patches uitgebracht voor de genoemde versies om de diverse kwetsbaarheden te verhelpen door verbeterde autorisatiecontroles, input- en outputvalidatie, en filtering van gevoelige data te implementeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-1-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-5796	5.3 MEDIUM
CVE-2026-5952	5.3 MEDIUM
CVE-2026-11379	2.3 LOW
CVE-2026-10712	5.3 MEDIUM
CVE-2026-0934	5.1 MEDIUM
CVE-2026-1606	5.3 MEDIUM
CVE-2026-3176	2.3 LOW
CVE-2026-10086	5.1 MEDIUM
CVE-2026-12053	6.9 MEDIUM
CVE-2026-8330	4.6 MEDIUM
CVE-2026-2238	6.9 MEDIUM
CVE-2026-12635	2.3 LOW
CVE-2026-5309	5.3 MEDIUM

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-350	Reliance on Reverse DNS Resolution for a Security-Critical Action
CWE-532	Insertion of Sensitive Information into Log File
CWE-639	Authorization Bypass Through User-Controlled Key

CWE-862	Missing Authorization
CWE-863	Incorrect Authorization

Getroffen producten

GitLab
Community Edition, Enterprise Edition

Disclaimer