Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0270

Kwetsbaarheden verholpen in GitLab door GitLab Inc.

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 30-07-2026

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, specifiek in versies voorafgaand aan 19.0.5, 19.1.3 en 19.2.1, inclusief GitLab Enterprise Edition (EE) versies binnen deze reeksen.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van GitLab:

- Onjuiste toegangcontrole waardoor geauthenticeerde gebruikers met gastrechten testrapporten konden inzien die beperkt hadden moeten zijn.
- Onvoldoende validatie van gebruikersinvoer waardoor geauthenticeerde gebruikers de CI/CD pipeline schema's van andere gebruikers konden wijzigen.
- Onjuiste verwerking van upstream verzoeken in virtuele registries leidend tot mogelijke ongeautoriseerde informatielekken.
- Een raceconditie die het mogelijk maakte om de verplichte goedkeuringsworkflow te omzeilen en direct code te mergen in beschermde branches.
- Onvoldoende toegangscontrole bij interne verzoekverwerking waardoor ontwikkelaars toegang kregen tot informatie buiten hun autorisatie.
- Onvoldoende resource throttling bij het verwerken van merge request discussies, wat door niet-geauthenticeerde gebruikers misbruikt kon worden voor een denial-of-service.
- Onjuiste autorisatiecontroles op merge request samenwerking waardoor ontwikkelaars konden blijven committen na intrekking van hun toegang.
- Onjuiste autorisatie waardoor niet-geauthenticeerde gebruikers de titels van vertrouwelijke issues konden bekijken via publieke merge requests.
- Onjuiste verwerking van onbetrouwbare inhoud in de AI-assisted code review functie, wat toegang tot projectinformatie mogelijk maakte.
- Onvoldoende inputsanitatie waardoor cross-site scripting (XSS) aanvallen mogelijk waren via speciaal opgemaakte URLs.
- Onjuiste autorisatie tijdens token generatie waardoor geauthenticeerde gebruikers admin-governance policies konden omzeilen.
- Onjuiste API-toegangscontrole waardoor gebruikers met Maintainer rol beschermde branch instellingen konden wijzigen.
- Ontbrekende autorisatiecontrole waardoor niet-geautoriseerde gebruikers toegang kregen tot project import broninformatie. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde informatieontsluiting, manipulatie van workflows, omzeilen van beveiligingsmechanismen, denial-of-service en privilege escalatie binnen de GitLab omgeving.

Oplossingen

GitLab Inc. heeft updates uitgebracht voor GitLab versies voorafgaand aan 19.0.5, 19.1.3 en 19.2.1, inclusief GitLab Enterprise Edition, om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-4672	4.3 MEDIUM
CVE-2026-12436	8.4 HIGH
CVE-2026-16553	5.4 MEDIUM
CVE-2026-13113	6.5 MEDIUM
CVE-2026-6267	8.5 HIGH
CVE-2026-15975	7.5 HIGH
CVE-2025-14562	3.1 LOW
CVE-2026-14351	4.3 MEDIUM
CVE-2026-15077	4.3 MEDIUM
CVE-2026-3093	4.7 MEDIUM
CVE-2026-15831	4.3 MEDIUM
CVE-2026-14341	4.9 MEDIUM
CVE-2026-6336	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-522	Insufficiently Protected Credentials
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes
CWE-1230	Exposure of Sensitive Information Through Metadata
CWE-1270	Generation of Incorrect Security Tokens
CWE-1427	Improper Neutralization of Input Used for LLM Prompting

Getroffen producten

GitLab
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.