Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0168

## Kwetsbaarheden verholpen in GitLab Community Edition en Enterprise Edition

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 28-05-2026

**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 heeft meerdere kwetsbaarheden verholpen in GitLab Community Edition en Enterprise Edition, specifiek in versies 12.7 tot voor 18.10.7, 18.11 tot voor 18.11.4, en 19.0 tot voor 19.0.1.

## Duiding

De kwetsbaarheden betreffen verschillende aspecten van authenticatie, autorisatie en validatie binnen GitLab. Een denial of service kan worden veroorzaakt door onvoldoende validatie, waarbij een geauthenticeerde gebruiker de beschikbaarheid van de dienst kan verstoren. Daarnaast kunnen gebruikers met developer-permissies ongeautoriseerd toegang krijgen tot gevoelige deploymentdata door onjuiste autorisatiecontroles. Verder is er een probleem met onjuiste gebruikersidentiteitsresolutie, waardoor een geauthenticeerde gebruiker Duo AI-workflows kan activeren alsof hij een andere gebruiker is, wat leidt tot identiteitsvervalsing binnen deze workflows. Ook kunnen developer-rollen flowbeperkingen omzeilen die op groepsniveau zijn ingesteld, wat de toegangscontrole en workflow governance beïnvloedt. Een andere kwetsbaarheid maakt het mogelijk voor onbevoegde gebruikers om private projecten te enumereren, wat kan leiden tot blootstelling van gevoelige projectinformatie. Ten slotte kunnen geauthenticeerde gebruikers toegang krijgen tot continuous integration (CI) data die niet voor hen bedoeld is, door een fout in de toegangscontrole voor CI-data.

De kwetsbaarheid met kenmerk CVE-2026-2710 wordt wel genoemd in de releasenotes van GitLab, maar is ingetrokken en heeft geen verdere impact.

## Oplossingen

GitLab heeft updates uitgebracht in de genoemde versies om de diverse kwetsbaarheden te verhelpen door validatie- en autorisatielogica te corrigeren en de gebruikersidentiteitsresolutie te verbeteren. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- https://about.gitlab.com/releases/2026/05/27/patch-release-gitlab-19-0-1-released/

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2026-1402 | 6.5 MEDIUM |
| CVE-2026-2601 | 4.3 MEDIUM |

| | |
|---|---|
| CVE-2026-4868 | 8.2 HIGH |
| CVE-2026-5296 | 4.3 MEDIUM |
| CVE-2026-6713 | 5.3 MEDIUM |
| CVE-2026-8716 | 4.3 MEDIUM |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-639 | Authorization Bypass Through User-Controlled Key |
| CWE-706 | Use of Incorrectly-Resolved Name or Reference |
| CWE-770 | Allocation of Resources Without Limits or Throttling |
| CWE-862 | Missing Authorization |
| CWE-863 | Incorrect Authorization |

## Getroffen producten

| **GitLab** |
|---|
| GitLab |

## Disclaimer