Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0128

Kwetsbaarheden verholpen in GitLab EE en CE

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-04-2026

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 en Enterprise Edition, specifiek in versies variërend van 9.2 tot voor 18.11.1, inclusief diverse 18.x releases.

Duiding

De kwetsbaarheden betreffen verschillende componenten van GitLab, waaronder de discussions endpoint, GraphQL API, note retrieval, issue import, Mermaid sandbox, Storybook development environment, issue rendering, web interface en Virtual Registries. Geauthenticeerde gebruikers kunnen door onvoldoende resource limits of onjuiste inputvalidatie resource-exhaustie veroorzaken, wat leidt tot Denial-of-Service. Daarnaast zijn er problemen met onjuiste autorisatiecontroles waardoor project owners group fork preventie kunnen omzeilen, en met onvoldoende CSRF-bescherming waardoor ongeauthenticeerde gebruikers GraphQL mutaties kunnen uitvoeren. Verder is er een cross-site scripting (XSS) kwetsbaarheid die ongeauthenticeerde gebruikers toestaat om JavaScript code in de browser van een gebruiker uit te voeren. Ook kunnen gebruikers door onjuiste toegangscontrole de titels van vertrouwelijke issues in publieke projecten inzien en toegang krijgen tot Virtual Registries via onjuist gescopeerde credentials. Sommige kwetsbaarheden maken het mogelijk om ongeautoriseerde content te injecteren in browser sessies van andere gebruikers. De kwetsbaarheden zijn aanwezig in meerdere opeenvolgende versies en betreffen zowel Community als Enterprise edities van GitLab.

Oplossingen

GitLab Inc. heeft updates en patches uitgebracht in versies vanaf 18.9.6, 18.10.4 en 18.11.1 om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://about.gitlab.com/releases/2026/04/22/patch-release-gitlab-18-11-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-0186	6.5 MEDIUM
CVE-2025-3922	6.5 MEDIUM
CVE-2025-6016	6.5 MEDIUM
CVE-2025-9957	2.7 LOW

CVE-2026-1660	6.5 MEDIUM
CVE-2026-3254	3.5 LOW
CVE-2026-4922	8.1 HIGH
CVE-2026-5262	8.0 HIGH
CVE-2026-5377	4.3 MEDIUM
CVE-2026-5816	8.0 HIGH
CVE-2026-6515	5.4 MEDIUM

CWE's

CWE	Beschrijving
CWE-41	Improper Resolution of Path Equivalence
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-613	Insufficient Session Expiration
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-863	Incorrect Authorization
CWE-1021	Improper Restriction of Rendered UI Layers or Frames

Getroffen producten

GitLab
GitLab

Disclaimer