Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0003

Kwetsbaarheden verholpen in GitLab

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-01-2026

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 kwetsbaarheden verholpen in GitLab CE/EE.

Duiding

De kwetsbaarheden omvatten verschillende problemen, waaronder de mogelijkheid voor geauthenticeerde gebruikers om externe API-aanroepen te misbruiken, wat kan leiden tot een Denial-of-Service. Daarnaast konden geauthenticeerde gebruikers via GraphQL ongeautoriseerde wijzigingen aanbrengen in projectconfiguraties en AI-instellingen van ongeautoriseerde namespaces. Een andere kwetsbaarheid stelde ongeauthenticeerde gebruikers in staat om willekeurige code uit te voeren in de browser van een geauthenticeerde gebruiker via een kwaadaardige webpagina. Bovendien konden geauthenticeerde gebruikers gevoelige informatie lekken door speciaal vervaardigde afbeeldingen te gebruiken die de bescherming van de asset proxy omzeilden. Ten slotte was er een kwetsbaarheid die het mogelijk maakte om opgeslagen cross-site scripting (XSS) uit te voeren via GitLab Flavored Markdown, wat de beveiliging van de applicatie in gevaar kon brengen.

Oplossingen

GitLab heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://about.gitlab.com/releases/2026/01/07/patch-release-gitlab-18-7-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-10569	6.5 MEDIUM
CVE-2025-11246	5.4 MEDIUM
CVE-2025-13761	8.0 HIGH
CVE-2025-13772	7.1 HIGH
CVE-2025-13781	6.5 MEDIUM

CVE-2025-3950	3.5 LOW
CVE-2025-9222	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-862	Missing Authorization
CWE-1220	Insufficient Granularity of Access Control

Getroffen producten

GitLab
GitLab

Disclaimer