



NCSC-2025-0087

Kwetsbaarheden verholpen in GitLab

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-03-2025

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 EE/CE versies van 11.5 tot 17.9.2.

Duiding

De kwetsbaarheden omvatten onder andere een probleem waarbij gebruikers met aangepaste rechten meer lidmaatschapsverzoeken kunnen goedkeuren dan waar ze recht op hebben, wat kan leiden tot ongeautoriseerde toegang tot beperkte gebieden binnen het platform. Daarnaast zijn er kwetsbaarheden in de Google Cloud IAM-integratiefunctie die kwaadwillenden in staat kunnen stellen om kwaadaardige code in het systeem in te voeren. Er zijn ook kwetsbaarheden die gevoelige authenticatie-informatie kunnen blootstellen en een denial-of-service kunnen veroorzaken door manipulatie van specifieke invoer. Bovendien zijn er kritieke kwetsbaarheden in de ruby-saml-bibliotheek en de graphql-ruby-bibliotheek die kunnen leiden tot ongeautoriseerde toegang en remote code execution. Deze kwetsbaarheden vereisen onmiddellijke aandacht van beveiligingsbeheerders.

Oplossingen

GitLab heeft patches en updates uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://about.gitlab.com/releases/2025/03/12/patch-release-gitlab-17-9-2-released/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-7296	5.1 MEDIUM
➤ CVE-2024-8402	1.8 LOW
➤ CVE-2024-12380	2.1 LOW
➤ CVE-2024-13054	5.3 MEDIUM
➤ CVE-2025-0652	5.3 MEDIUM
➤ CVE-2025-1257	6.9 MEDIUM

> CVE-2025-25291	8.8 HIGH
> CVE-2025-25292	8.8 HIGH
> CVE-2025-27407	6.3 MEDIUM

CWE's

CWE	Beschrijving
> CVE-473	PHP External Variable Modification
> CVE-347	Improper Verification of Cryptographic Signature
> CVE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CVE-94	Improper Control of Generation of Code ('Code Injection')
> CVE-436	Interpretation Conflict
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-863	Incorrect Authorization
> CVE-209	Generation of Error Message Containing Sensitive Information

Getroffen producten

GitLab
Enterprise Edition
Community Edition, Enterprise Edition
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.