



NCSC-2025-0288

Kwetsbaarheden verholpen in GitLab CE/EE

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-09-2025

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 CE/EE (Versies voor 18.1.6, 18.2.6, en 18.3.2).

Duiding

De kwetsbaarheden in de getroffen versies stellen geauthenticeerde gebruikers in staat om tokenbeheer te manipuleren, achtergrondtaken te verstoren, meerdere grote SAML-antwoorden te verzenden, proxy-omgevingen te manipuleren, toegang te krijgen tot onderhoudsnotities die alleen voor beheerders zijn, en om excessief grote bestanden te uploaden. Dit kan leiden tot operationele inefficiënties, verstoring van de beschikbaarheid van het platform, ongeoorloofde blootstelling van gevoelige informatie en zelfs een aanhoudende denial-of-service. Beheerders moeten bijzonder waakzaam zijn voor ongebruikelijke activiteiten en ervoor zorgen dat de toegang tot gevoelige informatie goed wordt beheerd.

Oplossingen

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

Referenties

➤ <https://about.gitlab.com/releases/2025/09/10/patch-release-gitlab-18-3-2-released/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-10094	7.1 HIGH
➤ CVE-2025-1250	5.3 MEDIUM
➤ CVE-2025-2256	6.9 MEDIUM
➤ CVE-2025-6454	2.3 LOW
➤ CVE-2025-6769	5.3 MEDIUM
➤ CVE-2025-7337	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-918	Server-Side Request Forgery (SSRF)
> CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

GitLab
Community Edition, Enterprise Edition
GitLab
Open Source
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.