



NCSC-2026-0303

Kwetsbaarheden verholpen in GitLab door GitLab Inc.

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 25-08-2026

Revisie: 1.0.1

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

Update Revisie 1

Publieke PoC code beschikbaar en actief misbruik waargenomen.

Feiten

GitLab Inc. heeft kwetsbaarheden verholpen in GitLab Community Edition (CE) en Enterprise Edition (EE).

Duiding

De kwetsbaarheden bevinden zich in de GraphQL-implementatie van GitLab. Een eerste kwetsbaarheid maakte het mogelijk voor niet-geauthenticeerde gebruikers om via een GraphQL-directive ongeautoriseerde wijzigingen of verwijderingen uit te voeren op publieke projecten en gebruikersdata. Een tweede kwetsbaarheid stelde niet-geauthenticeerde gebruikers in staat om mutaties uit te voeren via GET-requests door onjuiste validatie van GraphQL multiplex queries, waarbij mutatie-operaties niet correct werden beperkt. Hierdoor kunnen onbevoegden ongeautoriseerde wijzigingen aanbrengen in de staat van de server.

Update: Inmiddels is er publieke PoC code beschikbaar waardoor de kans op actief misbruik aanzienlijk toeneemt. Het NCSC adviseert voor systemen waar dit nog niet gebeurt is zo snel mogelijk de updates door te voeren.

Oplossingen

GitLab Inc. heeft updates uitgebracht die deze kwetsbaarheden verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-4-released/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-19478	9.4 CRITICAL
➤ CVE-2026-19650	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-352	Cross-Site Request Forgery (CSRF)

Getroffen producten

GitLab
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.