Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0303

Kwetsbaarheden verholpen in GitLab door GitLab Inc.

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 18-08-2026

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 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.

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