Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0297

Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2026

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 heeft meerdere kwetsbaarheden verholpen in GitLab Enterprise Edition (EE) en Community Edition (CE) versies variërend van 12.0 tot en met 19.2.2.

Duiding

De kwetsbaarheden betreffen verschillende aspecten van GitLab, waaronder onjuiste privilege-toewijzing waarbij gebruikers met een pending lidmaatschapsstatus onbedoeld permissies konden erven van custom rollen.

Verder zijn er problemen met ontbrekende autorisatiecontroles op API-endpoints, waardoor gebruikers met ontwikkelaarsrollen toegang konden krijgen tot externe statuscheckconfiguraties en beperkte merge request informatie van private projecten.

Er is ook een Denial-of-Service mogelijk door onjuiste inputvalidatie, en cross-site scripting (XSS) kwetsbaarheden in de analytics dashboard component door onvoldoende sanitisatie van gebruikersinvoer.

Daarnaast konden gebruikers met lagere rechten bepaalde package registry metadata wijzigen en CI/CD pipelines op beschermde branches triggeren zonder de juiste permissies. Er waren ook autorisatieproblemen die het mogelijk maakten om project- en groepsinstellingen ongeautoriseerd te wijzigen, en een GraphQL query die toegang gaf tot beleidsconfiguraties van niet-toegestane namespaces.

Ten slotte was er een probleem met onjuiste autorisatie van identiteitinformatie, wat leidde tot verkeerde toewijzing van AI-gebruik aan andere namespaces.

Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang, wijziging van gegevens, privilege-escalatie, en verstoring van de beschikbaarheid binnen de GitLab Enterprise Edition omgeving.

Oplossingen

GitLab heeft updates en patches uitgebracht voor de genoemde versies om de diverse kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-2-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-9486	3.3 LOW
CVE-2026-4879	4.3 MEDIUM
CVE-2026-6821	4.3 MEDIUM
CVE-2026-7427	5.3 MEDIUM
CVE-2026-8667	4.3 MEDIUM
CVE-2026-15216	8.7 HIGH
CVE-2026-15217	8.7 HIGH
CVE-2026-15423	8.5 HIGH
CVE-2026-16494	7.1 HIGH
CVE-2026-16627	7.7 HIGH
CVE-2026-18244	4.3 MEDIUM
CVE-2026-18433	4.3 MEDIUM
CVE-2026-19228	8.5 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-266	Incorrect Privilege Assignment
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-862	Missing Authorization

CWE-863	Incorrect Authorization

Getroffen producten

GitLab
GitLab

Disclaimer