Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0300

Kwetsbaarheden verholpen in GitLab EE & CE

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 29-09-2025

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 (Specifiek voor versies voor 18.2.7, 18.3.3, en 18.4.1).

Duiding

De kwetsbaarheden omvatten onder andere de mogelijkheid voor geauthenticeerde gebruikers om vertrouwelijke informatie te benaderen door projecten met dezelfde naam als die van het slachtoffer te creëren, en het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie binnen virtuele registerconfiguraties. Daarnaast kunnen geauthenticeerde gebruikers een onbeschermde GraphQL API misbruiken, wat kan leiden tot een Denial-of-Service (DoS) situatie. Ook is er een privilege-escalatie kwetsbaarheid die het mogelijk maakt voor ontwikkelaars met specifieke rechten om ongeautoriseerde toegang te krijgen tot extra systeemcapaciteiten. Bovendien kunnen ongeauthenticeerde gebruikers een DoS-voorwaarde activeren door grote, speciaal gemaakte JSON-bestanden te uploaden. Tot slot is er een prestatieafname vastgesteld bij bepaalde versies van GitLab, wat de gebruikerservaring kan beïnvloeden.

Oplossingen

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

Referenties

- https://about.gitlab.com/releases/2025/09/25/patch-release-gitlab-18-4-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-5069	**5.1 MEDIUM**
CVE-2025-7691	**5.3 MEDIUM**
CVE-2025-8014	**6.9 MEDIUM**
CVE-2025-9642	**5.1 MEDIUM**
CVE-2025-9958	**5.3 MEDIUM**
CVE-2025-10858	**6.9 MEDIUM**

CVE-2025-10867	**5.1 MEDIUM**
CVE-2025-10868	**5.1 MEDIUM**
CVE-2025-10871	**5.1 MEDIUM**
CVE-2025-11042	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-267	Privilege Defined With Unsafe Actions
CWE-708	Incorrect Ownership Assignment
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-840	CWE-840
CWE-862	Missing Authorization
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

GitLab
Community Edition, Enterprise Edition
Enterprise Edition

Disclaimer