Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0390

Kwetsbaarheden verholpen in GitLab CE/EE

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-12-2025

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.

Duiding

De kwetsbaarheden omvatten verschillende problemen, waaronder de mogelijkheid voor geauthenticeerde gebruikers om kwaadaardige afbeeldingen te uploaden, ongeautoriseerde acties uit te voeren door het injecteren van kwaadaardige HTML, gevoelige informatie te verkrijgen via GraphQL-queries, en het omzeilen van WebAuthn tweefactorauthenticatie. Daarnaast kunnen ongeauthenticeerde gebruikers kwaadaardige scripts injecteren in de Swagger UI en GraphQL-querycomplexiteitslimieten misbruiken, wat kan leiden tot Denial of Service (DoS) situaties.

Oplossingen

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

Referenties

- https://about.gitlab.com/releases/2025/12/10/patch-release-gitlab-18-6-2-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-4097	6.5 MEDIUM
CVE-2025-8405	5.1 MEDIUM
CVE-2025-11247	4.3 MEDIUM
CVE-2025-11984	6.8 MEDIUM
CVE-2025-12029	8.0 HIGH
CVE-2025-12562	7.5 HIGH
CVE-2025-12716	5.1 MEDIUM
CVE-2025-12734	3.5 LOW

CVE-2025-13978	**4.3 MEDIUM**
CVE-2025-14157	**7.1 HIGH**

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
CWE-116	Improper Encoding or Escaping of Output
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

GitLab
Community Edition, Enterprise Edition
GitLab

Disclaimer