Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0377

Kwetsbaarheden verholpen in GitLab

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-11-2025

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 zijn Community Edition (CE) en Enterprise Edition (EE) versies.

Duiding

De kwetsbaarheden omvatten onder andere de mogelijkheid voor niet-geauthenticeerde gebruikers om Denial of Service (DoS) condities te veroorzaken door het indienen van kwaadaardige JSON-verzoeken. Daarnaast konden niet-geauthenticeerde gebruikers zich aansluiten bij willekeurige organisaties door verzoekheaders te wijzigen, wat leidde tot ongeautoriseerde toegang tot organisatorische middelen. Geauthenticeerde gebruikers konden ook ongeautoriseerde toegang krijgen tot gevoelige tokens uit bepaalde logs, wat verdere exploitatie mogelijk maakte. Bovendien konden geauthenticeerde gebruikers met specifieke rechten een Denial of Service-conditie veroorzaken via HTTP-responsverwerking. Tot slot was er een risico op ongeautoriseerde toegang tot beveiligingsrapportinformatie in bepaalde configuraties. Deze kwetsbaarheden vereisten onmiddellijke aandacht van de leverancier om de integriteit en beschikbaarheid van de getroffen systemen te waarborgen.

Oplossingen

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

Referenties

- https://about.gitlab.com/releases/2025/11/26/patch-release-gitlab-18-6-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-12571	6.9 MEDIUM
CVE-2025-12653	6.9 MEDIUM
CVE-2024-9183	
CVE-2025-13611	2.0 LOW
CVE-2025-7449	5.3 MEDIUM
CVE-2025-6195	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-290	Authentication Bypass by Spoofing
CWE-425	Direct Request ('Forced Browsing')
CWE-532	Insertion of Sensitive Information into Log File
CWE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

GitLab
Community Edition, Enterprise Edition

Disclaimer