Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0093

Kwetsbaarheden verholpen in GitLab

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-03-2026

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 kwetsbaarheden verholpen in versies 18.9.2, 18.8.6 en 18.7.6

Duiding

De kwetsbaarheden omvatten verschillende problemen, waaronder onjuiste autorisatiecontroles die geauthenticeerde gebruikers in staat stelden om toegang te krijgen tot gevoelige gegevens, zoals metadata van private repositories, en het mogelijk maken van denial-of-service situaties door onjuiste invoervalidatie. Specifieke kwetsbaarheden betroffen de CI/CD-pijplijn, webhook-verwerking, en de importfunctionaliteit, waarbij ongepaste toegang tot API-gegevens en projectmetadata kon optreden. De kwetsbaarheden beïnvloeden de vertrouwelijkheid en beschikbaarheid van gegevens binnen GitLab.

Oplossingen

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

Referenties

- https://about.gitlab.com/releases/2026/03/11/patch-release-gitlab-18-9-2-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-3848	5.0 MEDIUM
CVE-2025-12555	4.3 MEDIUM
CVE-2025-12576	6.5 MEDIUM
CVE-2025-12697	2.2 LOW
CVE-2025-12704	3.5 LOW
CVE-2025-13690	6.5 MEDIUM
CVE-2025-13929	7.5 HIGH
CVE-2025-14513	7.5 HIGH

CVE-2026-0602	4.3 MEDIUM
CVE-2026-1069	7.5 HIGH
CVE-2026-1090	8.7 HIGH
CVE-2026-1182	4.3 MEDIUM
CVE-2026-1230	4.1 MEDIUM
CVE-2026-1663	4.3 MEDIUM
CVE-2026-1732	4.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-116	Improper Encoding or Escaping of Output
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-674	Uncontrolled Recursion
CWE-706	Use of Incorrectly-Resolved Name or Reference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

GitLab
GitLab

Disclaimer