



NCSC-2025-0100

Kwetsbaarheden verholpen in GitLab EE/CE

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 27-03-2025

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 EE/CE (Specifiek voor versies van 13.5.0 tot 17.10.1).

Duiding

De kwetsbaarheden omvatten een invoervalidatiefout die het mogelijk maakt voor gebruikers om kwaadaardige code in CLI-opdrachten te injecteren, een cross-site scripting kwetsbaarheid die het mogelijk maakt voor kwaadwillenden om willekeurige scripts uit te voeren in de context van een gebruikerssessie, en een onjuist toegangscontroleprobleem dat downgraded instance beheerders in staat stelt om verhoogde privileges te behouden. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang en de integriteit van systemen en gebruikersrechten ondermijnen.

Oplossingen

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

Referenties

➤ <https://about.gitlab.com/releases/2025/03/26/patch-release-gitlab-17-10-1-released/>

Kwetsbaarheden

| CVE | CVSS Score |
|----------------------------------|------------|
| ➤ CVE-2024-9773 | 3.7 LOW |
| ➤ CVE-2024-10307 | |
| ➤ CVE-2024-12619 | |
| ➤ CVE-2025-0811 | 8.7 HIGH |
| ➤ CVE-2025-2242 | 7.5 HIGH |
| ➤ CVE-2025-2255 | 8.7 HIGH |

CWE's

| CWE | Beschrijving |
|---------------------------|--|
| ➤ CWE-77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| ➤ CWE-863 | Incorrect Authorization |
| ➤ CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

Getroffen producten

| |
|--------------------|
| GitLab |
| GitLab |
| Open Source |
| GitLab |

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.