



# NCSC-2024-0270

## Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 04-07-2024

Revisie: 1.0.1

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Update Revisie 1

Per abuis is er een kwetsbaarheid met kenmerk CVE-2024-5655 niet aan dit beveiligingsadvies toegevoegd. Deze is alsnog toegevoegd. Inschaling blijft ongewijzigd.

## Feiten

GitLab heeft kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, om gegevens in de repositories te manipuleren, of om met rechten van een andere gebruiker, waaronder ook mogelijk functioneel/technisch beheerders of teamleads, willekeurige commando's uit te voeren.

## Oplossingen

GitLab heeft updates uitgebracht om de kwetsbaarheden te verhelpen in GitLab EE en CE v 17.1.1, 17.0.3 en 16.11.5. Zie bijgevoegde referenties voor meer informatie.

## Referenties

➤ <https://about.gitlab.com/releases/2024/06/26/patch-release-gitlab-17-1-1-released/>

## Kwetsbaarheden

| CVE                             | CVSS Score |
|---------------------------------|------------|
| ➤ <a href="#">CVE-2024-1493</a> | 6.5 MEDIUM |
| ➤ <a href="#">CVE-2024-1816</a> | 5.5 MEDIUM |
| ➤ <a href="#">CVE-2024-2177</a> |            |
| ➤ <a href="#">CVE-2024-2191</a> | 5.3 MEDIUM |
| ➤ <a href="#">CVE-2024-3115</a> | 4.3 MEDIUM |
| ➤ <a href="#">CVE-2024-3959</a> | 6.5 MEDIUM |

|                 |              |
|-----------------|--------------|
| > CVE-2024-4011 | 4.3 MEDIUM   |
| > CVE-2024-4557 | 6.5 MEDIUM   |
| > CVE-2024-4901 | 8.7 HIGH     |
| > CVE-2024-4994 |              |
| > CVE-2024-5430 | 6.8 MEDIUM   |
| > CVE-2024-6323 | 7.5 HIGH     |
| > CVE-2024-5655 | 9.6 CRITICAL |

## CWE's

| CWE       | Beschrijving   |
|-----------|--|
| > CVE-200 | Exposure of Sensitive Information to an Unauthorized Actor                           |
| > CVE-284 | Improper Access Control  |
| > CVE-285 | Improper Authorization   |
| > CVE-400 | Uncontrolled Resource Consumption  |
| > CVE-653 | Improper Isolation or Compartmentalization   |
| > CVE-79  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

## Getroffen producten

|               |
|---------------|
| <b>gitlab</b> |
| 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.