Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0237

Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-05-2024

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

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service (DoS) te veroorzaken, of via een Cross-Site-Scripting-aanval (XSS) gevoelige gegevens te verzamelen om accounts over te nemen.

Oplossingen

GitLab heeft updates uitgebracht om de kwetsbaarheden te verhelpen in GitLab EE en CE 17.0.1, 16.11.3 en 16.10.6. Zie bijgevoegde referenties voor meer informatie.

https://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/

Referenties

- https://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-6502	4.3 MEDIUM
CVE-2023-7045	5.4 MEDIUM
CVE-2024-1947	4.3 MEDIUM
CVE-2024-2874	6.5 MEDIUM
CVE-2024-4835	8.0 HIGH
CVE-2024-5258	4.4 MEDIUM
CVE-2024-5318	4.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-284	Improper Access Control
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-400	Uncontrolled Resource Consumption
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

gitlab
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.