



NCSC-2024-0490

Kwetsbaarheden verholpen in GitLab

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-12-2024

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 GitLab CE/EE (Specifiek voor versies 11.0 tot 17.6.2).

Duiding

De kwetsbaarheden bevinden zich in verschillende versies van GitLab CE/EE en stellen aanvallers in staat om groepen te creëren met namen die overeenkomen met bestaande unieke domeinen, wat kan leiden tot domeinverwarring. Daarnaast kunnen gebruikers ongeautoriseerde toegang krijgen tot vertrouwelijke incidenttitels via de Wiki History Diff-functie, en kan er een injectie van NEL-headers plaatsvinden in Kubernetes proxy-responses, wat het risico op gegevensfiltratie vergroot. Bovendien kunnen gevoelige informatie in GraphQL-mutaties worden gelogd en bewaard, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens.

Oplossingen

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

Referenties

➤ <https://about.gitlab.com/releases/2024/12/11/patch-release-gitlab-17-6-2-released/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-8116	
➤ CVE-2024-8179	5.4 MEDIUM
➤ CVE-2024-8233	7.5 HIGH
➤ CVE-2024-8647	
➤ CVE-2024-8650	
➤ CVE-2024-9367	4.3 MEDIUM
➤ CVE-2024-9387	6.4 MEDIUM

> CVE-2024-9633	
> CVE-2024-10043	3.1 LOW
> CVE-2024-11274	8.7 HIGH
> CVE-2024-12292	4.0 MEDIUM

CWE's

CWE	Beschrijving
> CVE-708	Incorrect Ownership Assignment
> CVE-601	URL Redirection to Untrusted Site ('Open Redirect')
> CVE-532	Insertion of Sensitive Information into Log File
> CVE-863	Incorrect Authorization

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.