



NCSC-2024-0447

Kwetsbaarheden verholpen in GitLab CE/EE

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-11-2024

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 16.0 tot 17.5.2).

Duiding

De kwetsbaarheden bevinden zich in meerdere versies van GitLab CE/EE en stellen kwaadwillenden in staat om ongeautoriseerde volledige API-toegang te verkrijgen via de Device OAuth-stroom. Dit kan leiden tot ernstige implicaties voor organisaties die deze producten gebruiken, aangezien het de beveiliging van gevoelige gegevens en gebruikersaccounts compromitteert.

Daarnaast is er een kritieke kwetsbaarheid die gebruikers blootstelt aan XSS-aanvallen door onjuiste uitvoerencoding wanneer het Content Security Policy (CSP) niet is ingeschakeld. Ook kunnen kwaadwillenden kwaadaardige JavaScript injecteren in Analytics Dashboards via een speciaal gemaakte URL, wat kan leiden tot ongeautoriseerde toegang en manipulatie van gevoelige gegevens.

Tenslotte kan ongeautoriseerde toegang tot de Kubernetes-agent in specifieke configuraties mogelijk zijn, wat zorgen oproept over de integriteit en beveiliging van implementaties.

Oplossingen

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

Referenties

➤ <https://about.gitlab.com/releases/2024/11/13/patch-release-gitlab-17-5-2-released/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-7404	6.8 MEDIUM
➤ CVE-2024-8180	5.4 MEDIUM
➤ CVE-2024-8648	6.1 MEDIUM
➤ CVE-2024-9693	8.5 HIGH
➤ CVE-2024-10240	

CWE's

CWE	Beschrijving
CWE-1021	Improper Restriction of Rendered UI Layers or Frames
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.