Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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