Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0237

Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

2024-05-27 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

GitLab heeft kwetsbaarheden verholpen in Enterprise Edition (EE) en Community Edition (CE).

Interpretaties

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/