Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2025-0100

Kwetsbaarheden verholpen in GitLab EE/CE

2025-03-27 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 GitLab EE/CE (Specifiek voor versies van 13.5.0 tot 17.10.1).

Interpretaties

De kwetsbaarheden omvatten een invoervalidatiefout die het mogelijk maakt voor gebruikers om kwaadaardige code in CLI-opdrachten te injecteren, een cross-site scripting kwetsbaarheid die het mogelijk maakt voor kwaadwillenden om willekeurige scripts uit te voeren in de context van een gebruikerssessie, en een onjuist toegangscontroleprobleem dat downgraded instance beheerders in staat stelt om verhoogde privileges te behouden. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang en de integriteit van systemen en gebruikersrechten ondermijnen.

Oplossingen

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

Referenties

- https://about.gitlab.com/releases/2025/03/26/patch-release-gitlab-17-10-1-released/