Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0270

Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 04-07-2024
Revisie: 1.0.1

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

Update Revisie 1

Per abuis is er een kwetsbaarheid met kenmerk CVE-2024-5655 niet aan dit beveiligingsadvies toegevoegd. Deze is alsnog toegevoegd. Inschaling blijft ongewijzigd.

Feiten

GitLab heeft kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, om gegevens in de repositories te manipuleren, of om met rechten van een andere gebruiker, waaronder ook mogelijk functioneel/technisch beheerders of teamleads, willekeurige commando's uit te voeren.

Oplossingen

GitLab heeft updates uitgebracht om de kwetsbaarheden te verhelpen in GitLab EE en CE v 17.1.1, 17.0.3 en 16.11.5. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://about.gitlab.com/releases/2024/06/26/patch-release-gitlab-17-1-1-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-1493	6.5 MEDIUM
CVE-2024-1816	5.5 MEDIUM
CVE-2024-2177	
CVE-2024-2191	5.3 MEDIUM
CVE-2024-3115	4.3 MEDIUM
CVE-2024-3959	6.5 MEDIUM

CVE-2024-4011	4.3 MEDIUM
CVE-2024-4557	6.5 MEDIUM
CVE-2024-4901	8.7 HIGH
CVE-2024-4994	
CVE-2024-5430	6.8 MEDIUM
CVE-2024-6323	7.5 HIGH
CVE-2024-5655	9.6 CRITICAL

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-400	Uncontrolled Resource Consumption
CWE-653	Improper Isolation or Compartmentalization
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

gitlab
gitlab

Disclaimer