Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0196

Kwetsbaarheden verholpen in GitLab Enterprise Edition

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-06-2026

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 meerdere kwetsbaarheden verholpen in GitLab Community Edition en Enterprise Edition (EE) versies variërend van 12.0 tot voor 19.0.2, inclusief belangrijke releases zoals 17.x, 18.10.8, 18.11.5 en 19.0.2.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van GitLab CE & EE. Geauthenticeerde gebruikers met developer-permissies kunnen via de Analytics Dashboard interface willekeurige client-side code uitvoeren door onvoldoende sanitatie van gebruikersinput. Op de CI/CD Catalog pagina kan een denial of service (DoS) worden veroorzaakt door onjuiste inputsanitatie, waardoor de pagina onbeschikbaar raakt. Een DoS kan ook optreden door het uploaden van speciaal vervaardigde bestanden die leiden tot resource-uitputting, wat de GitLab service kan laten crashen of onresponsief maken. Verder kunnen geauthenticeerde gebruikers ongeautoriseerde toegang krijgen tot vertrouwelijke issuegegevens door onjuiste autorisatiecontroles. Developer-gebruikers kunnen verborgen merge requests wijzigen door gebrekkige autorisatie, en ook merge request diff views manipuleren door onjuiste verwerking van bestandsnamen, wat wijzigingen kan verbergen tijdens code reviews. Gebruikers met de Security Manager rol kunnen projectbeveiligingsinstellingen beheren ondanks dat deze functie uitgeschakeld is, door onjuiste autorisatie. Binnen Group SAML identity management kunnen group Owners de controle over andere groepsleden overnemen door onjuiste autorisatiecontroles. Ongeautoriseerde e-mailadressen kunnen aan accounts worden toegevoegd via onvoldoende inputsanitatie in groepsinstellingen. Tijdens repository-import kan onvoldoende validatie van secundaire URL's leiden tot het uitlezen van willekeurige bestanden op de Gitaly-server en toegang tot interne netwerkbronnen. Ten slotte kan een niet-geauthenticeerde gebruiker de GitLab Support Bot imiteren door het injecteren van arbitraire inhoud in Service Desk e-mailantwoorden, veroorzaakt door onjuiste verwerking van e-mailsjablonen.

Oplossingen

GitLab heeft updates uitgebracht om deze kwetsbaarheden in GitLab Enterprise Edition te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-0-2-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-10087	**5.1 MEDIUM**

CVE-2026-10733	5.3 MEDIUM
CVE-2026-1500	5.3 MEDIUM
CVE-2026-3553	2.3 LOW
CVE-2026-6269	5.3 MEDIUM
CVE-2026-6277	5.3 MEDIUM
CVE-2026-6552	5.1 MEDIUM
CVE-2026-6976	2.3 LOW
CVE-2026-7250	6.9 MEDIUM
CVE-2026-8589	2.0 LOW
CVE-2026-9204	2.3 LOW
CVE-2026-9694	2.1 LOW

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-153	Improper Neutralization of Substitution Characters
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-1021	Improper Restriction of Rendered UI Layers or Frames

Getroffen producten

GitLab
Community Edition, Enterprise Edition
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.