Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0522

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in GitLab Enterprise Edition

Publicatiedatum: 26-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

GitLab heeft meerdere kwetsbaarheden verholpen in GitLab Enterprise Edition (versies voorafgaand aan 19.4.11, 19.5.9 en 19.6.2).

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van GitLab Enterprise Edition.

- Zo kunnen gebruikers met de rol developer zichzelf goedkeuring geven voor merge requests, waardoor zij wijzigingen direct in beschermde branches kunnen samenvoegen zonder de vereiste goedkeuring.
- Daarnaast is een probleem opgelost waarbij een gebruiker met Maintainer-privileges via onjuiste sessiebehandeling in de dependency proxy authenticatie toegang kon krijgen tot sessiecookies van andere gebruikers.
- Verder konden gebruikers met fine-grained personal access tokens merge request suggesties en werkitems buiten hun toegestane scope lezen en toepassen.
- Er is ook een kwetsbaarheid in de continuous integration (CI) job permissies die het mogelijk maakte om gevoelige informatie van andere gebruikers te verkrijgen, specifiek bij GitLab-instanties met inkomende e-mail ingeschakeld.
- Meerdere denial-of-service (DoS) kwetsbaarheden zijn opgelost, onder andere door onbeperkte backtracking in reguliere expressies, ontbrekende server-side inputvalidatie op on-call rotatie waarden, en het ontbreken van resource limits in de error tracking integratie.
- Verder zijn kwetsbaarheden in OAuth URL-validatie en repository import functionaliteit verholpen, die het mogelijk maakten om server-side request forgery (SSRF) aanvallen uit te voeren op interne netwerkbronnen.
- Ook is een probleem met onvoldoende validatie in cluster agents opgelost, waardoor gebruikers met Maintainer-rechten ongeautoriseerde verzoeken naar interne netwerkservices konden sturen.
- Tenslotte is een zwakke hashfunctie in het merge request approval proces aangepakt, die het mogelijk maakte om goedkeuringen te omzeilen, en een input sanitization probleem in de Service Desk e-mailverwerking, waardoor ongeauthenticeerde gebruikers quick actions konden uitvoeren.

Oplossingen

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

Referenties

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-6-2-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-107633	4.3 MEDIUM
CVE-2026-119452	6.7 MEDIUM
CVE-2026-129982	4.2 MEDIUM
CVE-2026-131867	6.3 MEDIUM
CVE-2026-132102	5.3 MEDIUM
CVE-2026-132156	6.5 MEDIUM
CVE-2026-132794	4.3 MEDIUM
CVE-2026-132822	6.5 MEDIUM
CVE-2026-135221	6.3 MEDIUM
CVE-2026-135636	3.5 LOW
CVE-2026-16744	5.0 MEDIUM
CVE-2026-17194	5.7 MEDIUM
CVE-2026-81336	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-149	Improper Neutralization of Quoting Syntax
CWE-328	Use of Weak Hash
CWE-384	Session Fixation
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

GitLab
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.