



Advisory NCSC-2026-0414

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in GitLab

Publicatiedatum: 13-10-2026

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 delen. 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 kwetsbaarheden verholpen in GitLab Community Edition (CE) en Enterprise Edition (EE), specifiek in versies voorafgaand aan 19.2.8, 19.3.5 en 19.4.2.

Duiding

De kwetsbaarheden zijn aanwezig in verschillende onderdelen van GitLab, waaronder de CI/CD pipelineomgeving, autorisatiemechanismen, API, Kubernetes-integratie en package registry. Kwaadwillenden kunnen de kwetsbaarheden misbruiken voor het uitvoeren van willekeurige code, vergrijpen van ongeautoriseerde toegang tot gevoelige gegevens en het uitvoeren van cross-site-scripting-aanvallen.

De kwetsbaarheid met kenmerk CVE-2026-97229 heeft de hoogste CVSS3.1-score van 10.0 gekregen. Een ongeauthenticeerde kwaadwillende kan deze kwetsbaarheid misbruiken om via een malafide CI/CD-configuratie willekeurige code uit te voeren.

Oplossingen

GitLab heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen in versies 19.2.8, 19.3.5 en 19.4.2. Het NCSC adviseert om deze beveiligingsupdates op korte termijn te installeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-97229	10.0 CRITICAL
CVE-2026-92883	8.7 HIGH
CVE-2026-16301	8.5 HIGH
CVE-2026-14814	8.2 HIGH

CVE	CVSS Score
CVE-2026-81839	7.7 HIGH
CVE-2026-96893	7.3 HIGH
CVE-2026-101168	6.2 MEDIUM
CVE-2026-7767	5.8 MEDIUM
CVE-2026-16275	5.3 MEDIUM
CVE-2026-84284	5.3 MEDIUM
CVE-2026-85529	5.3 MEDIUM
CVE-2026-100755	4.6 MEDIUM
CVE-2026-14552	4.3 MEDIUM
CVE-2026-6567	4.3 MEDIUM
CVE-2026-104661	4.3 MEDIUM
CVE-2026-14210	4.3 MEDIUM
CVE-2026-105458	4.3 MEDIUM
CVE-2026-5954	4.2 MEDIUM
CVE-2026-92528	4.2 MEDIUM
CVE-2026-78335	4.2 MEDIUM
CVE-2026-100104	3.5 LOW
CVE-2026-82632	3.1 LOW
CVE-2026-103549	2.7 LOW
CVE-2026-9268	2.7 LOW

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-185	Incorrect Regular Expression
CWE-190	Integer Overflow or Wraparound
CWE-266	Incorrect Privilege Assignment

CWE	Beschrijving
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-532	Insertion of Sensitive Information into Log File
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-625	Permissive Regular Expression
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-1220	Insufficient Granularity of Access Control
CWE-1427	Improper Neutralization of Input Used for LLM Prompting

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 or 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.