



Advisory NCSC-2026-0447

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in GitLab door GitLab Inc.

Publicatiedatum: 22-10-2026

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 12 kwetsbaarheden verholpen in GitLab Community Edition (CE) en Enterprise Edition (EE). Eén kwetsbaarheid is als kritiek aangemerkt.

GitLab heeft een kwetsbaarheid verholpen in GitLab Community Edition en Enterprise Edition binnen de versies vanaf 7.0 tot bepaalde 19.x releases.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-110264 heeft een CVSS-score van 10,0 en betreft een integer overflow bij het compileren van een speciaal vervaardigde reguliere expressie. Onder bepaalde omstandigheden kan een niet-geauthenticeerde kwaadwillende de kwetsbaarheid op afstand misbruiken om willekeurige code op de GitLab-serveruit te voeren. De kwetsbaarheid treft GitLab-versies vanaf 7.0.

De kwetsbaarheden met kenmerk CVE-2026-15723 en CVE-2026-112212 zijn als High aangemerkt. CVE-2026-15723 kan door een geauthenticeerd aanvaller bij specifieke SAML- en LDAP-configuraties leiden tot overname van een bestaand account. CVE-2026-112212 betreft cache poisoning in OAuth/OIDC-discovery-endpoints en kan bepaalde authenticatiestromen omleiden naar een door een kwaadwillende beheerde server. De overige kwetsbaarheden kunnen onder meer leiden tot ongeautoriseerde toegang tot informatie en het omzeilen van toegangs- en beveiligingscontroles.

GitLab heeft twee detectieregels gepubliceerd waarmee beheerders van self-managed GitLab-installaties kunnen zoeken naar mogelijke exploitatiepogingen van CVE-2026-110264. GitLab meldt voornamelijk geen actief misbruik van de kwetsbaarheid.

Oplossingen

GitLab adviseert alle getroffen self-managed installaties zo snel mogelijk te upgraden naar een gepatchte versie. De kwetsbaarheden zijn verholpen in 18.11.13, 19.0.10, 19.1.9, 19.2.9, 19.3.6, 19.4.3 en 19.5.1. GitLab.com is reeds bijgewerkt. GitLab Dedicated-installaties met versie 19.3.5-internal0, 19.4.2-internal0 of later bevatten de beveiligingsupdates al.

Voor CVE-2026-110264 adviseert GitLab beheerders van self-managed installaties daarnaast de detectieregels “Onigmo native worker crash” en “Org mode render error burst” te gebruiken om te controleren op mogelijke exploitatiepogingen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-12664	6.8 MEDIUM
CVE-2026-13319	4.3 MEDIUM
CVE-2026-14288	3.1 LOW
CVE-2026-15723	8.2 HIGH
CVE-2026-16255	5.9 MEDIUM
CVE-2026-103515	2.7 LOW
CVE-2026-105711	3.5 LOW
CVE-2026-105777	4.3 MEDIUM
CVE-2026-110264	10.0 CRITICAL
CVE-2026-112212	7.5 HIGH
CVE-2026-112326	3.1 LOW
CVE-2026-112378	4.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-190	Integer Overflow or Wraparound
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-348	Use of Less Trusted Source

CWE	Beschrijving
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

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.