Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0480

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in GitLab

Publicatiedatum: 11-11-2026

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 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 een kwetsbaarheid verholpen in GitLab Community Edition (CE) en Enterprise Edition (EE).

Duiding

De kwetsbaarheid betreft een heap buffer overflow veroorzaakt door onjuiste verwerking van grote conflict-marker groottes in kwaadaardige repositories. Dit kan leiden tot heap corruptie of het crashen van de applicatie tijdens merge-operaties.

Oplossingen

GitLab heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen in versies 19.3.8, 19.4.6 en 19.5.4. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://gitlab.com/gitlab-org/git/-/work_items/814

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-105437	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow

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.