Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0367

Kwetsbaarheid verholpen in GitLab Community en Enterprise Editions

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 12-09-2026

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 een kwetsbaarheid verholpen in GitLab Community en Enterprise Editions.

Duiding

De kwetsbaarheid bevindt zich in de repository commits API, waarbij een path traversal mogelijk is. Hierdoor kunnen niet-geauthenticeerde gebruikers willekeurige bestanden op het systeem lezen. De oorzaak ligt in onjuiste path confinement gecombineerd met ontbrekende authenticatiecontroles in de API-endpoint.

CISA heeft CVE-2026-85706 opgenomen in de Known Exploited Vulnerabilities-catalogus en er is publieke exploitcode beschikbaar. Vooral internetbereikbare, zelfbeheerde GitLab-installaties lopen risico, omdat een aanvaller zonder inloggegevens gevoelige bestanden kan lezen. Werk kwetsbare systemen direct bij naar GitLab 19.1.8, 19.2.6, 19.3.2 of nieuwer en onderzoek de API-logs op verdachte verzoeken met parameters als file.path. Roteer mogelijk blootgestelde credentials wanneer aanwijzingen voor misbruik worden aangetroffen.

Controleer bijgevoegde referenties voor de laatste updates.

Oplossingen

GitLab heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-85706	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-35	Path Traversal: '.../...//'
CWE-306	Missing Authentication for Critical Function

Getroffen producten

GitLab
Community Edition and Enterprise Edition
GitLab
Open Source
GitLab

Disclaimer