



# **AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE**

## **Përditësime të Sigurisë – GitLab AI Gateway**

Data: 10/02/2026

Version: 1.0

## Përmbajtja

Përmbledhje Ekzekutive .....	1
Informacione Teknike .....	1
Rekomandime .....	1
Referenca .....	1

### Përmbledhje Ekzekutive

---

GitLab ka publikuar përditësime kritike sigurie për GitLab AI Gateway për të adresuar një dobësi serioze që prek instalimet GitLab Duo Self-Hosted. Defekti lidhet me **zgjerimin e pasigurt të template-ve të input-it të furnizuar nga përdoruesi**, çka mund të çojë në DoS ose ekzekutim arbitrar kodi në AI Gateway. Shfrytëzimi me sukses mund të rezultojë në **komprometim të plotë të shërbimit të prekur**.

### Informacione Teknike

---

#### Detaje të Dobësisë

- **CVE:** CVE-2026-1868
- **CVSS Score:** 9.9 (Kritike)
- **Komponenti i prekur:** Duo Workflow Service (GitLab AI Gateway)
- **Përshkrim teknik:** Komponenti Duo Workflow Service nuk trajton në mënyrë të sigurt zgjerimin e template-ve të të dhënave të furnizuara nga përdoruesi në përkufizime të formuara posaçërisht të *Duo Agent Platform Flow*. Një sulmues i autentikuar mund ta shfrytëzojë këtë dobësi për të shkaktuar DoS ose për të arritur ekzekutim arbitrar kodi në AI Gateway.
- **Ndikimi:** Mund të rezultojë në komprometim të plotë të shërbimit.

#### Versionet e Prekura

- **GitLab AI Gateway:**
  - Të gjitha versionet nga **18.1.6**, **18.2.6** dhe **18.3.1**
  - Përpara versioneve **18.6.2**, **18.7.1** dhe **18.8.1**

#### Versionet e Rregulluara

- **GitLab AI Gateway 18.6.2**
- **GitLab AI Gateway 18.7.1**
- **GitLab AI Gateway 18.8.1**

### Rekomandime

---

AKSK rekomandon përditësimin e menjëhershëm të versioneve të prekura në versionet e rregulluara ose më të fundit të publikuara nga GitLab.

### Referenca

---

<https://about.gitlab.com/releases/2026/02/06/patch-release-gitlab-ai-gateway-18-8-1-released/>