GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 September 2026

Advisory 309: GitLab Enterprise Edition Duo Chat GraphQL Deserialization Leading to Credential Disclosure (CVE-2026-87719).

Release Date: 12th September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate a self-managed GitLab Enterprise Edition (EE) instance with Duo Chat enabled. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-87719 is a critical insecure-deserialization vulnerability in GitLab Enterprise Edition, disclosed on 12 September 2026 in the same patch release that fixed CVE-2026-85706 (Advisory 302, GitLab's unauthenticated repository-commits-API path traversal).

CERTVU's Advisory 302 noted this CVE for context but deliberately did not build it as an independent advisory, since it requires authenticated Duo Chat access - a fundamentally different, narrower attack surface than CVE-2026-85706's fully unauthenticated flaw.

What are the systems affected?

The following version(s) are affected:

- GitLab Enterprise Edition (EE) 18.3 through 19.1.7, 19.2.0 through 19.2.5, and 19.3.0 through 19.3.1 - (Affected)

GitLab EE 19.1.8, 19.2.6, and 19.3.2 and later – (Not affected, patched); GitLab Community Edition (CE), GitLab.com, and GitLab Dedicated - (Not affected)

Upgrade self-managed GitLab Enterprise Edition to 19.1.8, 19.2.6, or 19.3.2 (matching your current release line).

What does this mean?

Typical attack flow:

1. **Use an authenticated account with Duo Chat access to craft a malicious GraphQL subscription argument**
    - An attacker who already holds an authenticated GitLab EE account with Duo Chat access crafts a GraphQL subscription argument designed to bypass the application's serialization protections.
2. **Perform an unauthorized server-side object lookup and obtain sensitive credentials**
    - The crafted argument allows the attacker to perform unauthorized server object lookups, gaining access to Advanced Search configuration data and other sensitive credentials stored on the instance.

Attack vectors:

- A network-based attack against any self-managed GitLab EE instance, requiring the attacker to already hold an authenticated account with Duo Chat access - a materially narrower precondition than Advisory 302's fully unauthenticated companion flaw.
- No user interaction is required beyond the attacker's own crafted request (CVSS UI:N), though low privileges (specifically, Duo Chat access) are required (CVSS PR:L). CERTVU found no report of confirmed active exploitation or public proof-of-concept code for this CVE at the time of writing.

Successful exploitation may allow attackers to:

- Perform unauthorized server-side object lookups on a GitLab EE instance using only an account with Duo Chat access.
- Obtain Advanced Search configuration data and other sensitive credentials, and use them to pivot further into the organization's GitLab-connected infrastructure.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch

- Upgrade self-managed GitLab Enterprise Edition to 19.1.8, 19.2.6, or 19.3.2 (matching your current release line). Confirm whether your instance is also affected by CVE-2026-85706

(Advisory 302), which shares the same patch release but has a materially more urgent, unauthenticated attack path.

2. Review and restrict Duo Chat access where patching must be delayed
3. Audit for signs of prior misuse before and after patching
4. Rotate credentials accessible via Advanced Search configuration

Report any suspected compromise of a GitLab instance to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-87719
2. https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/