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 302: GitLab Repository Commits API Unauthenticated Path Traversal Leading to Arbitrary File Read - Actively Exploited (CVE-2026-85706).

Release Date: 11th 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 Community Edition (CE) or Enterprise Edition (EE) instance. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85706 is a critical, unauthenticated path traversal vulnerability in the repository commits API of GitLab, one of the world's most widely-used DevOps and source-code management platforms, used extensively by software development organizations, government agencies, and enterprises globally to host and manage source code. Improper path confinement combined with missing authentication enforcement in the "/api/v4/projects/{id}/repository/commits/" endpoint allows a remote, unauthenticated attacker to submit a single crafted HTTP request with a manipulated "file.path" parameter and read arbitrary files from the GitLab server - including SSH keys, database credentials, deploy tokens, CI/CD variables, and other sensitive configuration data.

What are the systems affected?

The following version(s) are affected:

- GitLab CE/EE 18.7 through 19.1.7 - (Affected)

- GitLab CE/EE 19.2.0 through 19.2.5, and 19.3.0 through 19.3.1 - (Affected)

GitLab CE/EE 19.1.8, 19.2.6, and 19.3.2 and later - (Not affected, patched); GitLab.com and GitLab Dedicated – (Already patched, no customer action required)

What does this mean?

Typical attack flow:

1. **Send a single crafted, unauthenticated HTTP request**
    - A remote, unauthenticated attacker sends an HTTP request to the GitLab repository commits API endpoint, "/api/v4/projects/{id}/repository/commits/", with a manipulated "file.path" parameter designed to escape the intended directory.
2. **Read arbitrary files from the GitLab server**
    - Due to improper path confinement and missing authentication enforcement on this endpoint, the request succeeds without any credentials, returning the contents of arbitrary files on the server - potentially including SSH keys, database credentials, deploy tokens, and CI/CD variables.

Attack vectors:

- A network-based, unauthenticated attack against any self-managed GitLab CE/EE instance reachable from an untrusted network, most critically the public internet.
- No user interaction or privileges are required (CVSS AV:N/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Read arbitrary files from the GitLab server without any authentication, using a single HTTP request.
- Obtain SSH keys, database credentials, deploy tokens, CI/CD variables, and other sensitive configuration data, and use them to pivot further into the organization’s source code, infrastructure, and deployment pipelines.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

- Upgrade self-managed GitLab CE/EE to 19.1.8, 19.2.6, or 19.3.2 (matching your current release line) as an emergency change, not scheduled maintenance, given confirmed active exploitation.

2. Restrict network access to the GitLab instance where patching must be delayed
3. Audit for signs of prior compromise before and after patching
4. Rotate credentials and secrets stored on or reachable from the GitLab instance

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-2026-85706
2. https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/