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

27 August 2026

Advisory 197: CVE-2026-60004_Gitea Code Injection Vulnerability

Release Date: 25th August 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 utilize the above products. This alert is intended to be understood by technical users and systems administrators.

Who should take note?

Gitea is a free, open-source, self-hosted Git platform used to store and manage source code repositories. Because it is free and runs on modest hardware, it is commonly deployed by:

- Software development and ICT service companies
- Tertiary and technical education institutions
- Government agencies and their software contractors
- Telecommunications operators and Internet Service Providers
- Individual development teams

CERTVU draws particular attention to that final category. Gitea is often installed informally by developers because it is free and quick to set up, and such instances may not appear on any organisational asset register. Organisations should not assume Gitea is absent simply because it was never formally procured.

What is it?

CVE-2026-60004 is a critical code injection vulnerability (CWE-94) in Gitea, a self-hosted Git service. It carries a CVSS Base Score of 9.8 and allows an attacker with ordinary repository write access to execute arbitrary shell commands as the operating system account running the Gitea service.
The flaw is in the diffpatch endpoint, which applies user-supplied patches within a temporary Git repository. Because the temporary repository was created as a bare clone, the repository directory itself acts as Git's internal data directory. A specially crafted patch can therefore cause attacker-controlled content to be written into the hooks directory as an executable Git hook.

What are the systems affected?

Self-hosted Gitea deployments on all supported operating systems, including Linux, Windows and container-based installations.

Gitea versions 1.17 through 1.27.0 - (Affected)
Gitea version 1.27.1 and later - (Not affected, patched)

What does this mean?

Although exploitation nominally requires an authenticated account, this offers far less protection than it appears. Gitea enables open user registration by default, so where that default has not been changed an external attacker can simply create an account, create a repository, and satisfy the write-access requirement without any prior access to the organisation.

Step 1 - Account Registration
An attacker, commonly an automated scanner, locates an internet-reachable Gitea instance and registers a user account. Where open registration is enabled without email confirmation or CAPTCHA, this step requires no human involvement.

Step 2 - Repository Creation
The attacker creates a repository under the newly registered account, thereby obtaining the repository write permissions the exploit requires.

Step 3 - Code Injection (CVE-2026-60004)
The attacker submits crafted patch content to the diffpatch endpoint. The patch causes an attacker-controlled executable file to be materialised as a Git hook within the temporary repository.

Step 4 - Command Execution and Payload Delivery
Git executes the hook during subsequent repository operations, running commands as the Gitea service account. Observed activity includes writing proof of code execution back into a Git branch, then downloading a shell loader and a cryptocurrency mining payload.

CERTVU assesses that the exploitation observed to date is opportunistic and automated rather than targeted. Attackers are scanning broadly for reachable Gitea instances without regard to the

organisation or country behind them. Vanuatu deployments are therefore exposed to the same scanning pressure as instances anywhere else, and should not be regarded as low priority on the basis of Vanuatu's size or location.

Mitigation process

CERTVU recommends the following:

1. **Determine Whether Gitea Is Present**

Establish first whether your organisation operates a Gitea instance at all, including any instance deployed by a development team outside central IT, and ask any external software contractor whether they run one.

2. **Disable Open Registration Immediately**

Where Gitea is present, disable open user registration without waiting for the update. This is the single highest-value immediate control, because it removes the mechanism by which an external attacker obtains the write access the exploit requires. Remove anonymous access and restrict repository write and API access to known users.

Mitigation option also include;

- Update to Gitea 1.27.1 or Later
- Restrict Network Exposure

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-60004
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://www.cisa.gov/news-events/alerts/2026/08/25/cisa-adds-one-known-exploited-vulnerability-catalog
4. https://www.helpnetsecurity.com/2026/08/26/gitea-cve-2026-60004-exploited-in-the-wild/
5. https://cwe.mitre.org/data/definitions/94.html