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

18 November 2026

Advisory 384: GPUStack Improper Authentication Vulnerability (CVE-2026-102895).

Release Date: 10th November 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 product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-102895 is a critical authentication bypass (CWE-287, CWE-290 and CWE-346) in GPUStack, an open-source tool for managing GPU clusters that serve AI models. Versions before 2.2.0 treat requests that appear to come from the local machine (loopback) as an administrator. Behind a reverse proxy, or when an attacker sets the X-Real-IP header, remote requests can appear local, giving unauthenticated attackers full administrator access. It is rated CVSS 9.8.

What are the systems affected?

The vulnerability affects:

- GPUStack versions before 2.2.0 (pip package gpustack and container images)
- Deployments behind a reverse proxy or reachable from the internet are at the highest risk

Not affected / patched version:

- GPUStack 2.2.0 or later; 2.2.2 or later also fixes CVE-2026-102894

What does this mean?

Successful exploitation may allow attackers to:

- Gain administrator access without logging in
- Create persistent administrator API keys and change users and models
- Read worker and cloud provider secrets
- Run code on GPU worker hosts through administrator features

Mitigation process

CERTVU recommends the following:

1. Upgrade GPUStack
Upgrade to GPUStack 2.2.2 or later, which fixes both CVE-2026-102895 and CVE-2026-102894.

2. Restrict access
3. Revoke keys and rotate secrets
4. Check for compromise

Report suspected compromise to CERTVU at incident@cert.gov.vu.

Reference

1. https://github.com/gpustack/gpustack/security/advisories/GHSA-gj9m-f8ph-pmhr
2. https://github.com/gpustack/gpustack/releases/tag/v2.2.0
3. https://www.cve.org/CVERecord?id=CVE-2026-102895
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-102895