

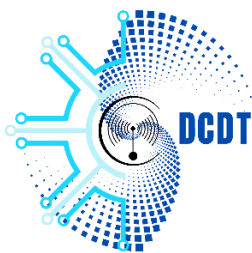
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

8 September 2026

Advisory 270: trycua cua-computer-server Missing Authentication for Critical Function (CVE-2026-86121).

Release Date: 5th 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, System/Network administrators, software development teams, and AI/ML engineering teams that use the open-source "cua" (Computer-Use Agent) platform, and specifically its computer-server component. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-86121 is a critical, unauthenticated remote code execution vulnerability in cua-computer-server, a core component of "cua," an open-source platform (over 22,200 GitHub stars, 1,500+ forks, backed by Y Combinator) that lets AI agents control real or virtualized desktop and OS environments across macOS, Windows, and Linux for automation, agent development, testing, and benchmarking. The computer-server component exposes a network API that lets an authorized client remotely drive a sandboxed computer instance - running commands, reading and writing files, and controlling mouse/keyboard input.

What are the systems affected?

The following version(s) are affected:

- cua-computer-server before 0.3.42 - (Affected)

cua-computer-server 0.3.42 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Reach the exposed computer-server network API**
 - Because an affected instance both skips authentication when CONTAINER_NAME is unset and binds to all network interfaces by default, any attacker able to reach the host on TCP port 8000 - over the local network, or directly from the internet if the host is exposed. This can connect to the service without presenting any credentials.
2. **Execute arbitrary commands and access the managed environment**
 - Once connected, the attacker can issue unauthenticated API requests to run arbitrary operating-system commands, read or write arbitrary files, and obtain an interactive shell on the environment the computer-server instance manages, which may be an isolated sandbox/VM, or, depending on how it was deployed, the underlying host machine itself.

Attack vectors:

- A network-based, unauthenticated attack against any reachable cua-computer-server instance where a developer workstation, a CI/CD runner, a cloud virtual machine, or shared AI-agent sandbox infrastructure is running an affected version with CONTAINER_NAME unset and the default network binding in place.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Gain arbitrary command execution and full control over the sandboxed computer instance — or, depending on deployment, the underlying host - that the cua-computer-server instance manages.
- Access any data, credentials, or source code present in the compromised sandbox or host, and use it as a foothold to pivot into a broader development, CI/CD, or AI-agent infrastructure network.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update cua-computer-server to version 0.3.42 or later (current latest: 0.3.45) via pip, and confirm the installed version directly rather than assuming it has already updated.

2. Restrict network exposure as defence-in-depth, even after patching
3. Audit developer, CI/CD, and AI-agent sandbox environments for this component
4. Explicitly set the CONTAINER_NAME environment variable regardless of patch status
5. Review logs for unexpected connections to port 8000

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

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-86121>
2. <https://github.com/trycua/cua>