

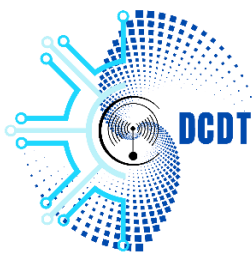
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 271: HKUDS AutoAgent TCP Command Server Unauthenticated Remote Code Execution (CVE-2026-86124).

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, and software development or AI/ML engineering teams that use HKUDS AutoAgent. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-86124 is a critical, unauthenticated remote code execution vulnerability in AutoAgent, an open-source "Fully-Automated and Zero-Code LLM Agent Framework" developed by HKUDS (the Data Intelligence Lab at the University of Hong Kong), with over 9,700 GitHub stars - comfortably within the adoption tier already established this session for open-source AI/developer infrastructure, alongside CAT (Advisory 258) and cua-computer-server (Advisory 270). developed products with no shared code or vendor relationship, so they are unrelated findings rather than companions, but the pattern is worth noting given how many organizations are now standing up similar AI-agent sandbox environments.

What are the systems affected?

The following version(s) are affected:

- HKUDS AutoAgent, all current versions/builds - (Affected)

What does this mean?

Typical attack flow:

1. **Reach the exposed TCP command server**
 - Because the sandbox's command server binds to all network interfaces by default and requires no authentication, any attacker able to reach a deployed AutoAgent instance on its exposed port can connect directly, without presenting any credentials.
2. **Execute arbitrary commands as root inside the sandbox, and potentially beyond it**
 - The attacker sends shell commands directly to the exposed command server, which executes them as root inside the container; because a host directory is bind-mounted into the container as writable, a successful attacker may also be able to affect files on the underlying host, escaping the intended sandbox isolation.

Attack vectors:

- A network-based, unauthenticated attack against any reachable AutoAgent sandbox instance: a developer workstation, a CI/CD runner, or a cloud host - with 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, root-level command execution inside the affected AutoAgent sandbox container.
- Leverage the container's writable bind-mounted host directory to affect files on the underlying host machine, effectively escaping the intended sandbox isolation, and use the compromised environment as a foothold into a broader development or AI infrastructure network.

Mitigation process

CERTVU recommends the following:

1. Restrict network exposure immediately - no vendor patch is currently available
 - Bind the command server and any other exposed AutoAgent ports to loopback (127.0.0.1) only rather than all interfaces, do not publish the container's command port beyond localhost, run the container as a non-root user where the framework allows it, and mount host directories read-only unless write access is specifically required. This is a workaround, not a fix. The underlying missing-authentication flaw remains present in the software.
2. Treat this as urgent alongside similar AI-agent sandbox tooling in the environment
3. Audit the estate for AutoAgent and similar AI-agent sandbox deployments
4. Monitor for a vendor fix and apply it once released
5. Consider isolating or decommissioning exposed instances if they cannot be adequately restricted

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

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-86124>
2. <https://github.com/HKUUDS/AutoAgent>