

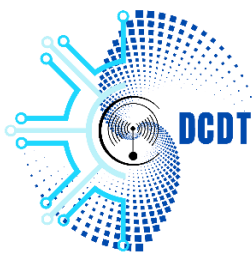
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 267: Tenda CP3 Kylin AlarmVoiceURL OS Command Injection (CVE-2026-86148).

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 general households or small businesses that use the Tenda CP3 Wi-Fi pan/tilt security camera. This alert is intended to be understood by both technical users and general consumers.

What is it?

CVE-2026-86148 is a critical OS command injection vulnerability in the Tenda CP3, the same consumer Wi-Fi pan/tilt security camera addressed in CERTVU Advisory 265 (CVE-2026-86152) and Advisory 266 (CVE-2026-86153), on the identical affected firmware build. CERTVU is issuing this as a separate advisory rather than combining it with the two prior ones, since Advisories 265 and 266 were already built and delivered before this third, distinct vulnerability was researched, and each affects a different function with a different underlying weakness. This flaw lies in the SystemAsh function of the device's Apis/system.c file, within the same Kylin component as Advisory 265's vulnerability: improper handling of the "AlarmVoiceURL" parameter allows a remote attacker to inject and execute arbitrary operating-system commands.

What are the systems affected?

The following version(s) are affected:

- Tenda CP3 firmware 27.5.57.101 - (Affected)

What does this mean?

Typical attack flow:

1. **Reach the camera's alarm-voice configuration function over the network**
 - A remote attacker sends a crafted request to a reachable Tenda CP3 device, supplying a malicious value for the "AlarmVoiceURL" parameter handled by the SystemAsh function of the device's Kylin component.
2. **Inject and execute arbitrary operating-system commands**
 - Because the affected function fails to properly sanitise the "AlarmVoiceURL" parameter before passing it to the underlying operating system, the attacker's injected command is executed directly on the device, giving the attacker arbitrary command execution.

Attack vectors:

- A network-based attack against any Tenda CP3 device reachable by the attacker, whether from the local home/business network or, on a device with remote access or port-forwarding enabled, directly from the internet.
- No user interaction is required (CVSS UI:N).

Successful exploitation may allow attackers to:

- Execute arbitrary commands on the affected camera, gaining full control of the device.
- Access the camera's live video and audio feed and its alarm/notification functionality, and use the compromised device as a foothold into the wider home or business network it is connected to - the same consequences already described for the companion vulnerability in Advisory 265.

Mitigation process

CERTVU recommends the following:

1. Restrict network access to the camera immediately - no vendor patch is currently available
 - Ensure the CP3 is not directly reachable from the internet (disable any remote-access or port-forwarding configuration exposing it), and where possible place it on an isolated guest or IoT-only network segment, separate from computers and other sensitive devices. This is a workaround, not a fix - the underlying command-injection flaw remains present in the firmware, and is the same workaround already recommended for Advisories 265 and 266.

2. Treat this as urgent alongside its companion vulnerabilities CVE-2026-86152 (Advisory 265) and CVE-2026-86153 (Advisory 266) on the same device
3. Audit the estate/household for Tenda CP3 and similar consumer camera deployments
4. Monitor for a vendor fix and apply it once released
5. Consider replacing the device if it cannot be adequately isolated

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

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-86148>
2. <https://www.tendacn.com/product/CP3v3>