

**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 265: Tenda CP3 Kylin Component Unauthenticated OS Command Injection (CVE-2026-86152).

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-2026-86152 is a maximum-severity, unauthenticated remote OS command injection vulnerability in the Tenda CP3, a consumer Wi-Fi pan/tilt security camera marketed for home and small-business monitoring (including as a baby monitor and pet camera) and sold globally through Amazon, general electronics retailers, and international-shipping platforms — unlike an ISP-provisioned device, it requires no specific local telecom infrastructure and can be purchased and connected to any home or business Wi-Fi network by any consumer.

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 Kylin service over the network**
 - A remote attacker sends a crafted request to a reachable Tenda CP3 device, targeting the CAutoAddWifi::ThreadProc function of the device's Kylin component, without needing to authenticate or interact with a legitimate user of the camera.
2. **Inject and execute arbitrary operating-system commands**
 - Because the affected function fails to properly sanitise its input, the attacker's request is passed to the underlying operating system and executed directly, giving the attacker arbitrary command execution on the camera with no prior access or credentials of any kind.

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, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/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 - a particularly sensitive consequence for a device marketed as a home or baby monitor and use the compromised device as a foothold into the wider home or business network it is connected to.

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.
2. Treat this as unpatched: Tenda had not released a fixed firmware version or formal advisory addressing this CVE at the time of writing
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-2026-86152>
2. <https://www.tendacn.com/product/CP3v3>