

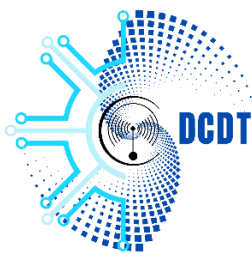
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 266: Tenda CP3 Redirect.cpp Improper Privilege Management (CVE-2026-86153).

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-2026-86153 is a critical improper privilege management vulnerability in the Tenda CP3, the same consumer Wi-Fi pan/tilt security camera addressed in CERTVU Advisory 265 (CVE-2026-86152), on the identical affected firmware build. CERTVU is issuing this as a separate advisory rather than combining it with Advisory 265, since Advisory 265 was already built and delivered before this second, distinct vulnerability was researched, and the two affect different functions with different underlying weaknesses.

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 redirect-management function over the network**
 - A remote attacker sends a crafted request to a reachable Tenda CP3 device, targeting the CRedirServer::SetRedirectEnable function, which does not properly verify that the caller holds the privilege level the function requires.
2. **Bypass the intended privilege restriction**
 - Because the function's privilege check is improperly implemented, the attacker's request is processed as though it came from a suitably privileged caller, allowing the attacker to enable or disable the device's redirect functionality and gain a level of control over the device that should have been restricted.

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). CERTVU is not aware of a public exploit or confirmed active exploitation at the time of writing, and EPSS scores this as a low near-term exploitation probability, but the device's status as a security/monitoring camera and its companion, more easily-exploitable vulnerability (CVE-2026-86152/Advisory 265) on the same firmware make it a priority for the same mitigation.

Successful exploitation may allow attackers to:

- Bypass the intended privilege restriction on the camera's redirect functionality, gaining a level of device control that should have required proper authorization.
- Manipulate the device's network redirect behaviour as an unauthorized user, and potentially combine this with other weaknesses on the same device - including CVE-2026-86152 - to further compromise the camera or the 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 privilege-management flaw remains present in the firmware.

2. Treat this as urgent alongside its companion CVE-2026-86152 (Advisory 265) 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-2026-86153>
2. <https://www.tendacn.com/product/CP3v3>