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

4 September 2026

Advisory 260: TOTOLINK CP450 cstecgi.cgi Buffer Overflow (CVE-2026-85031).

Release Date: 3rd 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, Internet Service Providers, and System/Network administrators that deploy the TOTOLINK CP450 outdoor wireless access point/CPE, including any operator using it to deliver wireless broadband links. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85031 is a critical buffer overflow vulnerability in the TOTOLINK CP450, a 5GHz outdoor wireless access point/client (CPE) device by TOTOLINK, a global consumer and small-ISP networking hardware vendor, marketed for long-range point-to-point and point-to-multipoint wireless links of the kind used by wireless internet service providers (WISPs) and rural broadband operators. The flaw lies in the device's web-management interface, in an unspecified function of /cgi-bin/cstecgi.cgi, where manipulation of the "topicurl" argument triggers a buffer overflow.

What are the systems affected?

The following version(s) are affected:

- TOTOLINK CP450 firmware 4.1.0 - (Affected)

What does this mean?

Typical attack flow:

1. **Obtain low-level access to the device's management interface**
    - An attacker obtains, guesses, or otherwise acquires low-level (non-administrative) credentials to the CP450's web-based management interface — for example, a default or weak password on a device that has not been reconfigured after deployment, or a shared/lower-tier account used by field technicians.
2. **Trigger the buffer overflow via a crafted request**
    - The attacker sends a specially crafted request to /cgi-bin/cstecgi.cgi with a malicious "topicurl" argument, overflowing a fixed-size buffer and potentially allowing arbitrary code execution on the device with the privileges of the web-server process.

Attack vectors:

- A network-based attack against any TOTOLINK CP450 device whose management interface is reachable by the attacker, whether from the local wireless link, the wider local network, or the internet if the interface is exposed.
- Only low-level privileges are required, no user interaction is needed, and attack complexity is low (CVSS AV:N/AC:L/PR:L/UI:N). A proof-of-concept exploit is already publicly available, which typically shortens the window before opportunistic scanning begins, though CERTVU is not aware of confirmed active exploitation at the time of writing.

Successful exploitation may allow attackers to:

- Execute arbitrary code on the affected CP450 device, potentially gaining full control of the wireless access point/CPE and any traffic it carries.
- Use a compromised CP450 as a foothold into the wider network it serves — including, for a WISP or rural-broadband operator, the connections of every downstream customer relying on that link — and disrupt or intercept the wireless service it provides.

Mitigation process

CERTVU recommends the following:

1. Restrict access to the device's management interface immediately — no vendor patch is currently available

- Ensure the CP450's web-management interface is reachable only from a trusted management network, never directly from the internet or the general wireless service area, and disable remote management if it is not strictly required. This is a workaround, not a fix — the underlying buffer overflow remains present in the firmware.

2. Treat this as unpatched: TOTOLINK had not released a fixed firmware version or formal advisory addressing this CVE at the time of writing
3. Audit the estate for TOTOLINK CP450 and related deployments
4. Replace default or weak credentials on every affected device
5. Monitor for a vendor fix and apply it once released

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-85031
2. https://www.totolink.net/product/CP450