

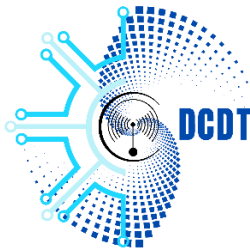
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

9 September 2026

**Advisory 282: Tenda AC18 Telnet Handler Missing Authentication Vulnerability
(CVE-2026-82695).**

Release Date: 31st August 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 members of the general public that use a Tenda AC18 wireless router. This alert is intended to be understood by both technical and general readers.

What is it?

CVE-2026-82695 is a missing-authentication vulnerability in the Telnet Handler component of the Tenda AC18, a mass-market AC1900-class dual-band Wi-Fi router sold through general electronics retailers worldwide (Amazon, eBay, and other consumer retail channels), with no dependency on any specific ISP.

What are the systems affected?

The following version(s) are affected:

- Tenda AC18 firmware 15.03.05.19 - (Affected)

No fixed firmware version currently available - (Not applicable)

What does this mean?

Typical attack flow:

1. **Reach the device's Web UI endpoint**
 - A remote attacker with network access to the router - over the local network, or directly from the internet if the Web UI is exposed - sends a crafted request to /goform/telnet without presenting any credentials.
2. **Enable Telnet and gain control**
 - Because the affected function performs no authentication check, the attacker's request is processed as if authenticated, enabling Telnet access to the device and allowing unauthorized administrative-level control, using the publicly available proof-of-concept exploit.

Attack vectors:

- A network-based, unauthenticated attack against any reachable Tenda AC18's Web UI, using publicly available exploit code.
- No user interaction and no privileges are required (CVSS AV:N/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Gain unauthenticated administrative-level control of the affected router via enabled Telnet access.
- Use a compromised router as a foothold to intercept, redirect, or manipulate the network traffic of every device connected behind it, or as a launch point for further attacks.

Mitigation process

CERTVU recommends the following:

1. Restrict access to the device's Web UI
 - Disable remote/WAN-side administration and Telnet access, and restrict access to the Web UI to trusted local devices only.
2. Monitor for a vendor firmware update
3. Consider replacement if no patch is released
4. Segment consumer networking devices from sensitive systems

Report any suspected compromise of a Tenda AC18 device, or unusual network behaviour on a network using one, to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-82695>
2. <https://cve.threatint.com/CVE/CVE-2026-82695>