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

14 September 2026

Advisory 306: TOTOLINK A3002MU Boa Web Server Multiple Unauthenticated Buffer Overflow Vulnerabilities - No Vendor Patch Available (CVE-2026-90605 and CVE-2026-90606).

Release Date: 12th 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/Wireless Service Providers, and individual consumers that operate a TOTOLINK A3002MU wireless router. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-90605 and CVE-2026-90606 are two critical, unauthenticated buffer overflow vulnerabilities in the Boa web server component of the TOTOLINK A3002MU, an AC1200 dual-band Gigabit wireless router marketed (including under a VPN-circumvention use case) as a mass-market consumer product, sold directly to individual consumers through general retail with no ISP dependency. CERTVU has previously judged TOTOLINK relevant to Vanuatu on this basis for other models in the product line (see Advisory 260, TOTOLINK CP450, and Advisory 280, TOTOLINK NR1800X). CVE-2026-90605 affects the "formFilter" function via the "ip6addr" parameter; CVE-2026-90606 affects the "formIpv6Setup" function via the "static_ipv6" parameter - both in the router's web management interface.

What are the systems affected?

The following version(s) are affected:

- TOTOLINK A3002MU, firmware Hh-B20211125.1046 (the newest available firmware for this model at time of writing) - (Affected)

No fixed firmware exists for either CVE-2026-90605 or CVE-2026-90606 at the time of writing

No official patch is available for either vulnerability. Organizations and consumers running an affected TOTOLINK A3002MU should apply the network-level mitigations below and evaluate replacing the device with an actively-supported model if it must remain in service long-term.

What does this mean?

Typical attack flow:

1. **Reach the router's web management interface with a crafted request**
    - A remote, unauthenticated attacker sends a specially crafted HTTP request to a reachable A3002MU's Boa web server - either to the "formFilter" endpoint with a manipulated "ip6addr" parameter (CVE-2026-90605), or to the "formIpv6Setup" endpoint with a manipulated "static_ipv6" parameter (CVE-2026-90606).
2. **Trigger a buffer overflow and execute arbitrary code or crash the device**
    - The oversized parameter overflows a fixed-size buffer in the Boa web server, potentially allowing the attacker to execute arbitrary code on the router or crash the device, without any authentication.

Attack vectors:

- A network-based, unauthenticated attack against any TOTOLINK A3002MU router with its web management interface reachable from an untrusted network, most critically the public internet or a shared/guest network segment.
- No user interaction or privileges are required for either flaw. CERTVU is not aware of confirmed active exploitation for either CVE at the time of writing, but public proof-of-concept exploit code exists for both, and the absence of any vendor fix means every affected device remains at standing risk indefinitely.

Mitigation process

CERTVU recommends the following:

1. Restrict access to the router's web management interface

- Since no vendor patch exists for either vulnerability, disable remote/WAN-side administration and restrict the web management interface to trusted local devices only, ensuring it is never directly reachable from the internet.

2. Place the device behind a firewall or on a segmented network
3. Evaluate replacing the device
4. Monitor for unauthorized activity on the network

Report any suspected compromise of a TOTOLINK router to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-90605
2. https://www.cve.org/CVERecord?id=CVE-2026-90606