

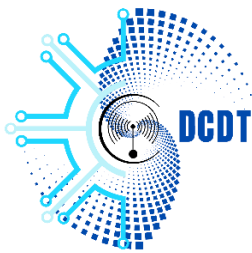
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 280: TOTOLINK NR1800X setUploadSetting Stack-Based Buffer
Overflow (CVE-2026-82616).**

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 TOTOLINK NR1800X 5G/LTE Wi-Fi 6 router. This alert is intended to be understood by both technical and general readers.

What is it?

CVE-2026-82616 is a critical stack-based buffer overflow in the setUploadSetting function of the file /cgi-bin/cstecgi.cgi on the TOTOLINK NR1800X, a mass-market, SIM-card-based 5G/LTE Wi-Fi 6 router sold through general electronics retailers internationally (including Amazon and multiple European and African online retailers), with no dependency on a specific local ISP or fixed-line service - any individual with a compatible mobile SIM can purchase and deploy one.

What are the systems affected?

The following version(s) are affected:

- TOTOLINK NR1800X firmware 9.1.0u.6681_B20230703 - (Affected)

No fixed firmware version currently available - (Not applicable)

What does this mean?

Typical attack flow:

1. **Reach the device's web-management CGI endpoint**
 - An attacker with low-level access to the device's web-management interface - for example, on the same network, or via a low-privileged account - sends a crafted request to `/cgi-bin/cstecgi.cgi` invoking `setUploadSetting` with an oversized `FileName` argument.
2. **Trigger the overflow and execute code**
 - The oversized argument overflows a stack buffer, allowing the attacker to execute arbitrary code on the device or crash it outright, using the publicly available proof-of-concept exploit.

Attack vectors:

- A network-based attack against any reachable TOTOLINK NR1800X's web-management interface, requiring only low-level access to that interface (CVSS PR:L) - a low bar that includes, for example, guessing or reusing a weak/default management password, or reaching the interface from an untrusted network segment.
- No user interaction is required, and a public exploit already exists

Successful exploitation may allow attackers to:

- Execute arbitrary code on the affected router, or crash it and disrupt the internet connectivity of any home, small office, or organization relying on it.
- Use a compromised router as a foothold to intercept, redirect, or manipulate the network traffic of every device connected behind it.

Mitigation process

CERTVU recommends the following:

1. Restrict access to the device's web-management interface
 - Disable remote/WAN-side administration and restrict access to the management interface to trusted local devices only; change any default or weak management credentials immediately.
2. Monitor for a vendor firmware update
3. Consider replacement if no patch is released
4. Segment IoT and consumer networking devices from sensitive systems
5. Report suspected compromise

Report any suspected compromise of a TOTOLINK NR1800X 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-2026-82616>
2. <https://radar.offsec.com/threat/cve-2026-82616-stack-based-buffer-overflow-in-totolink-nr1800x-6c42a25faadab882>