

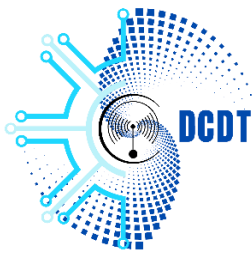
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 284: D-Link DIR-825M LTE Firmware Upgrade Stack-Based Buffer Overflow (CVE-2026-82593).

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 D-Link DIR-825M wireless router. This alert is intended to be understood by both technical and general readers.

What is it?

CVE-2026-82593 is a stack-based buffer overflow in the LTE Module Firmware Upgrade component of the D-Link DIR-825M, a mass-market wireless router with an LTE fallback/upgrade path, sold through general electronics retailers, with no dependency on a specific fixed-line ISP.

What are the systems affected?

The following version(s) are affected:

- D-Link DIR-825M firmware 1.1.8 - (Affected)

No fixed firmware version currently available - (Not applicable)

What does this mean?

Typical attack flow:

1. **Reach the device's LTE firmware-upgrade function**
 - An attacker with low-level access to the router's web-management interface sends a crafted request to /boafrm/formLtefotaUpgradeFibocom with an oversized "fota_url" value.
2. **Trigger the overflow and execute code**
 - The oversized value overflows a stack buffer in the function sub_41802C, allowing the attacker to execute arbitrary code on the device or crash it outright, using the publicly documented exploit technique.

Attack vectors:

- A network-based attack against any reachable D-Link DIR-825M's web-management interface, requiring only low-level access to that interface (CVSS PR:L).
- 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 consumer networking devices from sensitive systems

Report any suspected compromise of a D-Link DIR-825M 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-2026-82593>
2. https://github.com/Robots10/IoT_vlu/blob/main/reports/Dlink/formLtefotaUpgradeFibocom/formLtefotaUpgradeFibocom.md