



NOTICE

MCMC Advisory – Important Security Notice for D-Link Router Users (CVE-2025-29635)

CYBERJAYA, 29 APRIL 2026 – The Malaysian Communications and Multimedia Commission (MCMC) wishes to inform the public of an ongoing cyber threat targeting certain D-Link DIR-823X routers.

The vulnerability, identified as CVE-2025-29635, may allow attackers to gain unauthorised access and take control of affected routers remotely. The threat involves a Mirai-based malware campaign which may exploit outdated or unsupported devices connected to the internet.

Devices that are not updated may be exposed to the following security risks:

- Unauthorised access and control of the router
- Installation of malware on the device
- Enrolment into botnets used for cyberattacks
- Participation in distributed denial-of-service (DDoS) attacks

What Users Should Do

MCMC strongly advises users to:

- Check whether a D-Link DIR-823X router is currently in use. If the device is currently in use, users are advised to replace it, as it is no longer supported
- Disable remote administration or WAN management features if not required
- Change default or weak administrator passwords immediately
- Restart the device and perform a factory reset if suspicious activity is observed
- Keep network devices updated with the latest firmware where available

MCMC encourages all users to practise safe digital habits, keep their devices updated, and rely only on information from official sources.