



## NOTIS

### **Notis Keselamatan MCMC – Notis Keselamatan Penting untuk Pengguna Penghala D-Link (CVE-2025-29635)**

**CYBERJAYA, 29 April 2026** – Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC) ingin memaklumkan kepada orang awam mengenai ancaman keselamatan siber yang sedang berlaku yang menyasarkan beberapa penghala D-Link DIR-823X.

Kerentanan yang dikenal pasti sebagai CVE-2025-29635 berpotensi membolehkan penyerang mendapatkan akses tanpa kebenaran dan mengambil alih kawalan ke atas penghala yang terjejas secara jarak jauh. Ancaman ini melibatkan kempen perisian hasad berasaskan Mirai yang mengeksploitasi peranti yang tidak dikemas kini atau tidak lagi disokong yang disambungkan ke internet.

Peranti yang tidak dikemas kini mungkin terdedah kepada risiko keselamatan berikut:

- Akses tanpa kebenaran dan kawalan terhadap penghala
- Pemasangan perisian hasad pada peranti
- Penyertaan dalam botnet yang digunakan untuk serangan siber
- Penglibatan dalam serangan penafian perkhidmatan teragih (DDoS)

#### **Tindakan yang Perlu Diambil oleh Pengguna**

MCMC menasihati pengguna untuk:

- Menyemak sama ada peranti penghala D-Link DIR-823X sedang digunakan. Sekiranya peranti tersebut sedang digunakan, pengguna disarankan untuk menggantikannya kerana ia tidak lagi disokong
- Menyahaktifkan fungsi pentadbiran jarak jauh atau pengurusan WAN sekiranya tidak diperlukan
- Menukar kata laluan pentadbir lalai atau yang lemah dengan segera
- Memulakan semula dan melakukan tetapan semula kilang (factory reset) sekiranya terdapat aktiviti mencurigakan

- Mengemas kini peranti rangkaian dengan perisian tegar (firmware) terkini sekiranya tersedia

MCMC menggalakkan semua pengguna untuk mengamalkan amalan keselamatan siber yang baik, memastikan peranti sentiasa dikemas kini, dan hanya merujuk kepada maklumat daripada sumber rasmi.

**[www.mcmc.gov.my](http://www.mcmc.gov.my)**