TLP:CLEAR

# เอกสารการแจ้งเตือนกรณีพบช่องโหว่หลายรายการใน D-Link Wireless Router

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี D-Link ได้ออกอัปเดตเพื่อแก้ไขช่องโหว่หลายรายการ (CVE-2024-45694, CVE-2024-45695, CVE-2024-45696, CVE-2024-45697, CVE-2024-45698) โดยมีช่องโหว่ระดับ Critical จำนวน 3 รายการที่ส่งผลกระทบต่อ wireless router โดยมีรายละเอียดของช่องโหว่ดังต่อไปนี้[1]

- CVE-2024-45694 และ CVE-2024-45695 คะแนน (CVSSv3:9.8) เป็นช่องโหว่ Stack-Based Buffer Overflow ซึ่งทำให้ผู้โจมตีจากระยะไกลที่ไม่ได้รับการยืนยันตัวตนสามารถ Arbitrary Code Execution ได้
- CVE-2024-45696 คะแนน (CVSSv3:8.8) เป็นช่องโหว่ที่ทำให้ผู้โจมตีจากระยะไกลที่ไม่ได้รับการยืนยันตัวตนสามารถเปิดบริการ Telnet และเข้าสู่ระบบด้วย Hard-Coded Credentials ใน Local Network
- CVE-2024-45697 คะแนน (CVSSv3:9.8) เป็นช่องโหว่ที่ทำให้ผู้โจมตีจากระยะไกลที่ไม่ได้รับการยืนยันตัวตนสามารถเข้าถึงอุปกรณ์ที่ได้รับผลกระทบ และสามารถ Execute Operation System Commands ด้วย Hard-Coded Credentials
- CVE-2024-45698 คะแนน (CVSSv3:8.8) เป็นช่องโหว่ Input Validation ทำให้ผู้โจมตีจากระยะไกลสามารถเข้าถึง Telnet ด้วย Hard-Coded Credentials และ Execute Arbitrary OS Commands บนอุปกรณ์ที่ได้รับผลกระทบ[2]

ช่องโหว่ส่งผลกระทบต่อผลิตภัณฑ์ดังต่อไปนี้

- COVR-X1870 เวอร์ชัน v1.02 และก่อนหน้า
- DIR-X4860 เวอร์ชัน v1.04B04_Hot-Fix และก่อนหน้า
- DIR-X5460 เวอร์ชัน v1.11B01_Hot-Fix และก่อนหน้า

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

**อ้างอิง**


1. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-118
2. https://www.bleepingcomputer.com/news/security/d-link-fixes-critical-rce-hardcoded-password-flaws-in-wifi-6-routers/


TLP:CLEAR