TLP:CLEAR

เอกสารการแจ้งเตือนกรณีพบช่องโหว่ในเราเตอร์ D-Link ถูกใช้ประโยชน์ในการโจมตี

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีพบช่องโหว่ในเราเตอร์ D-Link ถูกใช้ประโยชน์ จำนวน 2 รายการ ได้แก่ DIR-600 และ DIR-605[1] โดยมีรายการช่องโหว่มีดังนี้

– CVE-2014-100005 (CVSS score: 6.8) [3] เป็นช่องโหว่ Cross-Site Request Forgery (CSRF) ที่ส่งผลกระทบต่อเราเตอร์ D-Link DIR-600[2] ซึ่งทำให้ผู้ไม่หวังดีสามารถเปลี่ยนการตั้งค่าเราเตอร์ได้โดยการขโมยเซสชันของผู้ดูแลระบบ

– CVE-2021-40655 (CVSS score: 7.5) [4] เป็นช่องโหว่ในการเปิดเผยข้อมูล (Information Disclosure) ส่งผลกระทบต่อเราเตอร์ D-Link DIR-605 ที่อนุญาตให้ผู้ไม่หวังดีสามารถได้รับชื่อผู้ใช้และรหัสผ่านของเราเตอร์ได้โดยการปลอมแปลงคำขอ HTTP POST ไปยังหน้า getcfg.php[2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานหรือผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบควรเลือกใช้ผลิตภัณฑ์รุ่นใหม่ตามคำแนะนำของผู้จำหน่าย ควรหลีกเลี่ยงการใช้ผลิตภัณฑ์ที่สิ้นสุดการสนับสนุน (End of Support - EOS) หรือสิ้นสุดอายุการใช้งาน (End of Life - EOL) เพื่อป้องกันการถูกใช้ในการโจมตี และควรตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ หรือตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้นและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ 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-2024-058
2. https://thehackernews.com/2024/05/cisa-warns-of-actively-exploited-d-link.html
3. https://nvd.nist.gov/vuln/detail/CVE-2014-100005
4. https://nvd.nist.gov/vuln/detail/CVE-2021-40655