แจ้งเตือน : ช่องโหว่

High

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนพบช่องโหว่ในเราเตอร์ D-Link บางรุ่น อาจถูกใช้ประโยชน์ในการโจมตี

วันที่แจ้งเตือน 4 มิถุนายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ทุกแห่ง

ThaiCERT สกมช. ได้เผยแพร่การพบช่องโหว่ในเราเตอร์ D-Link DIR-605 และ D-Link-DIR-600 ที่อาจถูกใช้ประโยชน์ ซึ่งสำนักงาน ก.ล.ต. พิจารณาแล้ว เห็นว่าอาจมีผู้ประกอบธุรกิจบางกลุ่มที่ใช้เราเตอร์ระดับ Home Use ในการดำเนินธุรกิจ ให้บริการกับลูกค้าหรือลักษณะเป็น shadow IT

ในการนี้ สำนักงาน ก.ล.ต. จึงขอแจ้งเตือนให้ผู้ประกอบธุรกิจในกลุ่มดังกล่าว ปรับปรุงแก้ไขช่องโหว่ ดังนี้ เพื่อความมั่นคงปลอดภัยขององค์กรท่านโดยรวม

(1) CVE-2021-40655 (CVSS score: 7.5) เป็นช่องโหว่ของเราเตอร์ D-Link DIR-605 ที่อนุญาตให้ผู้ไม่หวังดีสามารถได้รับชื่อผู้ใช้และรหัสผ่านของเราเตอร์ (Information Disclosure) ได้ โดยการปลอมแปลงคำขอ HTTP POST ไปยังหน้า getcfg.php

(2) CVE-2014-100005 (CVSS score: 6.8) เป็นช่องโหว่ Cross-Site Request Forgery (CSRF) ของเราเตอร์ D-Link DIR-600 ซึ่งทำให้ผู้ไม่หวังดีสามารถเปลี่ยนการตั้งค่าเราเตอร์ได้ โดยการขโมยเซสชันของผู้ดูแลระบบ

ทั้งนี้ ผู้ประกอบธุรกิจที่ใช้งานเราเตอร์ D-link รุ่นดังกล่าวควรหลีกเลี่ยงการใช้ผลิตภัณฑ์ที่สิ้นสุดการสนับสนุน (End of Support - EOS) หรือสิ้นสุดอายุการใช้งาน (End of Life - EOL) เพื่อป้องกันการถูกใช้ในการโจมตี และควรตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ

ผลกระทบจากการใช้ผลิตภัณฑ์ที่ EOS/EOL อาจนำไปสู่ความเสี่ยงด้านความมั่นคงปลอดภัยมากมาย เช่น ผู้ผลิตจะยุติการออกแพตช์หรืออัปเดตความปลอดภัย ทำให้ระบบมีความเสี่ยงต่อช่องโหว่ที่ถูกค้นพบใหม่และไม่ได้รับการแก้ไข ตกเป็นเป้าหมายของมัลแวร์ที่ออกแบบมาเพื่อใช้ประโยชน์จากช่องโหว่ที่ไม่ได้รับการแก้ไขโดยเฉพาะ เพิ่มความเสี่ยงในการถูกโจมตีและการรั่วไหลของข้อมูล เป็นต้น ดังนั้น ผู้ประกอบธุรกิจจึงควรตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจจะเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 27 พ.ค. 2567
2) https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-058
3) https://nvd.nist.gov/vuln/detail/CVE-2021-40655
4) https://nvd.nist.gov/vuln/detail/CVE-2014-100005