แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงในผลิตภัณฑ์ D-Link NAS ที่ End-of-Life (CVE-2024-10914)

วันที่แจ้งเตือน 15 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่กรณีพบช่องโหว่ร้ายแรงในอุปกรณ์จัดเก็บข้อมูลในเครือข่าย (Network-Attached Storage: NAS) ยี่ห้อ D-Link มากกว่า 60,000 เครื่อง ที่ End of Life: EoL (CVE-2024-10914) โดยผู้ไม่หวังดีอาศัยช่องโหว่ดังกล่าวส่งคำสั่งที่สร้างขึ้นเป็นพิเศษ (special crafted HTTP GET requests) เพื่อเข้าสู่อุปกรณ์ดังกล่าว และอาจส่งผลให้สามารถส่งมัลแวร์เข้าสู่ระบบได้

D-Link แนะนำให้ผู้ประกอบธุรกิจ หรือ ผู้ดูแลระบบที่ใช้งานที่ใช้ผลิตภัณฑ์ D-Link NAS ที่ EOL แล้ว ควรพิจารณาดำเนินการอย่างเหมาะสม เช่น พิจารณาแนวทางเลิกใช้งานอุปกรณ์ดังกล่าว ใช้งานผลิตภัณฑ์ที่ยังคงไม่สิ้นสุดการสนับสนุนโดยผู้ผลิต จำกัดการเข้าถึงต่ออุปกรณ์ดังกล่าว เป็นต้น

ผลิตภัณฑ์ที่ได้รับผลกระทบมีดังต่อไปนี้

- DNS-320 Version 1.00
- DNS-320LW Version 1.01.0914.2012
- DNS-325 Version 1.01, Version 1.02
- DNS-340L Version 1.08

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 14 พ.ย. 2567
2) https://nvd.nist.gov/vuln/detail/CVE-2024-10914
3) https://netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07