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

แจ้งเตือนช่องโหว่ในผลิตภัณฑ์ D-Link NAS ที่หมดอายุใช้งาน กำลังถูกใช้โจมตี

วันที่แจ้งเตือน 17 เมษายน 2567

ThaiCERT สกมช. ได้เผยแพร่ว่า D-Link ได้เปิดเผยช่องโหว่ 2 รายการ (CVE-2024-3272 และ CVE-2024-3273) ในอุปกรณ์ Network-Attached Storage (NAS) ดังนี้

- CVE-2024-3272 เป็นช่องโหว่ Backdoor ที่ทำให้ผู้โจมตีใช้ข้อมูลประจำตัว แบบฮาร์ดโค้ดเพื่อเข้าถึงอินเทอร์เฟซการจัดการเว็บโดยไม่ได้รับอนุญาต
- CVE-2024-3273 เป็นช่องโหว่ Command Injection ซึ่งอาจทำให้ผู้โจมตี สามารถ Arbitrary Command Execution บนระบบได้

ผลิตภัณฑ์ D-Link ที่ End of Life (EOL)/ End of Support (EOS) อาจได้รับผลกระทบจากช่องโหว่ดังกล่าว และแนะนำให้ผู้ประกอบธุรกิจหรือผู้ดูแลระบบที่ใช้งานที่ใช้ผลิตภัณฑ์ D-Link ที่ EOL/EOS ควรพิจารณาแนวทางที่เหมาะสม เช่น เลิกใช้งานอุปกรณ์และเปลี่ยนใช้งานอุปกรณ์ผลิตภัณฑ์ที่ยังคงสนับสนุนโดยผู้ผลิต เป็นต้น

ผลิตภัณฑ์ที่พบช่องโหว่	
DNS-120	DNS-326
DNR-202L	DNS-327L
DNS-315L	DNR-326
DNS-320	DNS-340L
DNS-320L	DNS-343
DNS-320LW	DNS-345
DNS-321	DNS-726-4
DNR-322L	DNS-1100-4
DNS-323	DNS-1200-05
DNS-325	DNS-1550-04

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 12 เม.ย. 2567
2) https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-039
3) https://nvd.nist.gov/vuln/detail/CVE-2024-3272
4) https://nvd.nist.gov/vuln/detail/CVE-2024-3273