TLP:CLEAR

เอกสารการแจ้งเตือนช่องโหว่ในผลิตภัณฑ์ D-Link NAS ที่หมดอายุใช้งาน กำลังถูกใช้โจมตี

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ พบผลิตภัณฑ์ D-Link ได้เปิดเผยช่องโหว่สองรายการ (CVE-2024-3272 และ CVE-2024-3273) ในอุปกรณ์ Network-Attached Storage (NAS)

- CVE-2024-3272 คะแนน CVSS 9.8 เป็นช่องโหว่ Backdoor ที่ทำให้ผู้โจมตีใช้ข้อมูลประจำตัวแบบฮาร์ดโค้ดเพื่อเข้าถึงอินเทอร์เฟซการจัดการเว็บโดยไม่ได้รับอนุญาต
- CVE-2024-3273 คะแนน CVSS 7.3 เป็นช่องโหว่ Command Injection ซึ่งอาจทำให้ผู้โจมตีสามารถ Arbitrary Command Execution บนระบบได้

ผลิตภัณฑ์ D-Link ที่ได้รับผลกระทบ End of Life (EOL) แนะนำให้ผู้ใช้และผู้ดูแลระบบที่ใช้งานผลิตภัณฑ์ที่ EOL ควรเลิกใช้งานอุปกรณ์และเปลี่ยนใช้งานอุปกรณ์ผลิตภัณฑ์ที่ยังคงสนับสนุนโดยผู้ผลิต

ทั้งนี้ ThaiCERT แนะนำให้หน่วยงานควรเฝ้าระวังความปลอดภัยและแพตช์ระบบสารสนเทศต่างๆ เป็นประจำป้องกันช่องโหว่ดังกล่าว รวมทั้งตรวจสอบการทำงานกิจกรรมต่าง ๆ ที่ผิดปกติและเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

<u>อ้างอิง</u>

1. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-039
2. https://arstechnica.com/security/2024/04/hackers-actively-exploit-critical-remote-takeover-vulnerabilities-in-d-link-devices/?utm_source=tldrinfosec

ช่องโหว่ส่งผลกระทบต่อผลิตภัณฑ์ต่อไปนี้	
ลำดับ	**ชื่อผลิตภัณฑ์**
1	DNS-120
2	DNR-202L
3	DNS-315L
4	DNS-320
5	DNS-320L
6	DNS-320LW
7	DNS-321
8	DNR-322L
9	DNS-323
10	DNS-325
11	DNS-326
12	DNS-327L
13	DNR-326
14	DNS-340L
15	DNS-343
16	DNS-345
17	DNS-726-4
18	DNS-1100-4
19	DNS-1200-05
20	DNS-1550-04