

ประจำวันพฤหัสบดีที่ 8 กันยายน 2565

ช่องโหว่ RCE ที่สำคัญส่งผลกระทบต่ออุปกรณ์ จัดเก็บข้อมูลเครือข่าย (NAS) ยี่ห้อ Zyxel

ผู้ผลิตอุปกรณ์เครือข่าย Zyxel ได้ออกแพทช์สำหรับแก้ไขช่องโหว่ด้านความปลอดภัยที่สำคัญซึ่งส่งผลกระทบต่ออุปกรณ์จัดเก็บข้อมูลเครือข่าย (NAS) ที่หมายเลขช่องโหว่ CVE-2022-34747 (คะแนน CVSS: 9.8) ปัญหานี้เกี่ยวข้องกับช่องโหว่ format string ที่ส่งผลกระทบต่อรุ่น NAS326, NAS540 และ NAS542 โดย Zyxel ให้เครดิตกับนักวิจัย Shaposhnikov Ilya สำหรับการรายงานถึงช่องโหว่นี้

บริษัทกล่าวว่าเมื่อวันที่ 6 กันยายน มีการพบช่องโหว่ของสตริงรูปแบบไบนารีเฉพาะของผลิตภัณฑ์ Zyxel NAS ที่อาจทำให้ผู้โจมตีสามารถดำเนินการจากระยะไกล โดยไม่ได้รับอนุญาตผ่านแพ็กเกจ UDP ที่สร้างขึ้น ช่องโหว่ที่ส่งผลกระทบมีรุ่นดังต่อไปนี้

- NAS326 (V5.21(AAZF.11)CO และรุ่นก่อนหน้า
- NAS540 (V5.21(AATB.8)CO และรุ่นก่อนหน้า
- NAS542 (V5.21(ABAG.8)CO และรุ่นก่อนหน้า

อุปกรณ์ NAS ถูกโจมตีมากขึ้นจนกลายเป็นเรื่องที่พบเจอบ่อยครั้ง หากใช้งานไม่ระมัดระวังหรือปรับปรุงซอฟต์แวร์ให้ทันสมัย อาจทำให้ผู้โจมตีสามารถขโมยข้อมูลสำคัญและข้อมูลส่วนตัว ในบางกรณีนั้นสามารถลบข้อมูลอย่างถาวรได้