ประจำวันอังคารที่ 20 กันยายน 2565

นักวิจัยเตือนถึงช่องโหว่ร้ายแรงใน Flexlan ที่ให้บริการ WiFi บนเครื่องบิน

นักวิจัยจาก Necrum Security Labs ค้นพบช่องโหว่ที่สำคัญ 2 ช่องโหว่ CVE–2022–36158 และ CVE–2022–36159 ซึ่งส่งผลกระทบต่ออุปกรณ์ LAN ของ Contec Flexlan FXA3000 และ FXA2000

โดยอุปกรณ์เหล่านี้ ติดตั้งอยู่บนเครื่องบินเพื่อใช้ในการเชื่อมต่ออินเทอร์เน็ตแก่ผู้โดยสาร ซึ่งผู้โจมตีสามารถใช้ช่องโหว่ข้างต้นเพื่อทำการเข้าควบคุมระบบ In-flight entertainment บนเครื่องบิน และอาจนำไปสู่การโจมตีที่เป็นอันตรายอื่นๆ โดยปัญหาที่ส่งผลกระทบกับอุปกรณ์ Contec FLEXLAN FXA3000 Series ตั้งแต่เวอร์ชัน 1.15.00 ลงมา และอุปกรณ์ FLEXLAN FXA2000 Series ตั้งแต่เวอร์ชัน 1.38.00 ลงมา

ช่องโหว่ CVE–2022–36158 เป็นหน้าเว็บคำสั่งระบบที่ซ่อนอยู่ซึ่งพบว่าทำ reverse engineering ของเฟิร์มแวร์ที่อุปกรณ์ใช้ หน้านี้ไม่ได้แสดงอยู่ในอินเทอร์เฟซ Wireless LAN Manager แต่อนุญาตให้เรียกใช้คำสั่ง Linux บนอุปกรณ์ที่มีสิทธิ์ของรูท เข้าถึงไฟล์ระบบทั้งหมด และเปิดพอร์ตเทลเน็ต ช่องโหว่ที่สอง CVE–2022–36159 เชื่อมโยงกับฮาร์ดโค้ด กุญแจรหัสที่อ่อนแอและบัญชีแบ็คดอร์ ผู้เชี่ยวชาญค้นพบไฟล์เงาที่มีแฮชของรูทและผู้ใช้

โดยนักวิจัยได้แนะนำให้เปลี่ยนรหัสผ่านผู้ใช้งานของบัญชีจากอินเทอร์เฟซผู้ดูแลเว็บและลบหน้าเว็บออกจากอุปกรณ์ และแนะนำให้สร้างรหัสผ่านที่แตกต่างกันสำหรับแต่ละอุปกรณ์

ที่มาของข่าว : https://securityaffairs.co/wordpress/135898/security/flexlan-critical-flaws.html