เอกสารการแจ้งเตือนกรณี Netgear เตือนช่องโหว่ในเราเตอร์ WiFi หลายรุ่น

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Netgear เตือนภัยช่องโหว่ในเราเตอร์ WiFi หลายรุ่น

Netgear ได้แจ้งเตือนถึงช่องโหว่ร้ายแรง 2 รายการ ที่ส่งผลกระทบต่อเราเตอร์ WiFi หลายรุ่น ได้แก่ PSV-2023-0039 และ PSV-2021-0117 โดยแนะนำให้ลูกค้าอัปเดตเฟิร์มแวร์ล่าสุดเพื่อป้องกันความเสี่ยงอย่างเร่งด่วน ช่องโหว่ทั้งสองประกอบไปช่องโหว่เรียกใช้โค้ดระยะไกล (Remote Code Execution) และช่องโหว่การหลีกเลี่ยงการตรวจสอบสิทธิ์ (Authentication Bypass) ซึ่งผู้โจมตีที่ไม่ได้รับการอนุญาตสามารถใช้ประโยชน์จากช่องโหว่เหล่านี้ได้โดยไม่จำเป็นต้องมีการตอบสนองใดๆ

1. ช่องโหว่ PSV-2023-0039 เป็นช่องโหว่ Remote Code Execution (RCE) ได้ส่งผลกระทบต่อเราเตอร์รุ่น XR1000, XR1000v2 และ XR500 และเวอร์ชันที่ได้รับการแก้ไข 1.0.0.74, 1.1.0.22 และ 2.3.2.134 ตามลำดับ

2. ช่องโหว่ PSV-2021-0117 Autentication Bypass ที่ช่วยให้ผู้โจมตี สามารถข้ามการตรวจสอบสิทธิ์และเข้าถึงการตั้งค่าเราเตอร์ ได้ส่งผลกระทบต่อเราเตอร์รุ่น WAX206, WAX220 และ WAX214v2 และเวอร์ชัน 1.0.5.3, 1.0.3.5 และ 1.0.2.5 ตามลำดับ[1]

โดยผู้ใช้สามารถดาวน์โหลดเฟิร์มแวร์ล่าสุดได้ผ่านทางเว็บไซต์ทางการของ Netgear โดยเข้าไปที่หน้าสนับสนุน (NETGEAR Support) และค้นหารุ่นของเราเตอร์ที่ใช้งานอยู่ จากนั้นเลือกดาวน์โหลดเฟิร์มแวร์เวอร์ชันล่าสุดภายใต้หัวข้อ "Current Versions" และทำตามคำแนะนำในการติดตั้งที่ระบุในคู่มือผู้ใช้หรือหน้า support ของผลิตภัณฑ์

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานดำเนินการดาวน์โหลดและติดตั้งเฟิร์มแวร์ล่าสุดทันทีเพื่อป้องกันการโจมตีที่อาจเกิดขึ้น และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://securityaffairs.com/173839/security/netgear-wifi-routers-flaws.html