เอกสารการแจ้งเตือนกรณีช่องโหว่ OpenVPN ทำให้ผู้โจมตีสามารถทำให้ระบบในเครื่องแม่ข่ายขัดข้องและสามารถถูกโจมตีจากระยะไกล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีช่องโหว่ OpenVPN ทำให้ผู้โจมตีสามารถทำให้ระบบในเครื่องแม่ข่ายขัดข้อง (Crash Server) และสามารถถูกโจมตีจากระยะไกล (Remote Code Execution : RCE)

ช่องโหว่ด้านความปลอดภัยใน OpenVPN ที่หมายเลข CVE-2025-2704 มีคะแนน CVSS: 5.9 ซึ่งอาจเปิดโอกาสให้ผู้โจมตีทำให้ระบบในเครื่องแม่ข่ายขัดข้อง ที่ส่งผลกระทบต่อเครื่องแม่ข่าย OpenVPN ตั้งแต่เวอร์ชัน 2.6.1 จนถึง 2.6.13 ซึ่งมีการกำหนดใช้งานด้วยคำสั่ง --tls-crypt-v2 โดยผู้โจมตีสามารถส่งข้อมูลแพ็กเก็ตบางส่วนหรือบางส่วนที่ผิดรูปแบบไปยังเครื่องแม่ข่ายเป้าหมาย ส่งผลให้สถานะไคลเอนต์ในเครื่องแม่ข่ายเกิดความเสียหาย และระบบจะเรียกใช้งานฟังก์ชันตรวจสอบภายใน (Self - Check) ซึ่งนำไปสู่การปิดการทำงานของเครื่องแม่ข่ายพร้อมข้อความแสดงข้อผิดพลาด ASSERT[1]

เพื่อความปลอดภัยของหน่วยงานหรือผู้ดูแลระบบที่ใช้ OpenVPN ควรดำเนินการดังต่อไปนี้[2]

- อัปเดตเป็น OpenVPN 2.6.14 ซึ่งเป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้ว[3]
- หากไม่สามารถอัปเดตได้ทันที ควรปิดการใช้งานตัวเลือก –tls-crypt-v2 เป็นการชั่วคราว แม้อาจจะส่งผลให้การป้องกันความเป็นส่วนตัวลดลง
- พิจารณาใช้การกรองแพ็กเก็ต (Packet filtering) และเฝ้าระวังบันทึก (logs) ของ VPN Server เพื่อหาสัญญาณความผิดปกติหรือความพยายามโจมตี

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://community.openvpn.net/openvpn/wiki/CVE-2025-2704
2. https://cybersecuritynews.com/openvpn-vulnerability-let-attackers-crash-servers/#google_vignette
3. https://openvpn.net/community-downloads/