เอกสารการแจ้งเตือนกรณี OpenSSL ออกแพตช์แก้ไขช่องโหว่ CVE-2024-12797 ป้องกันการโจมตีแบบ Man-in-the-Middle

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี OpenSSL ออกแพตช์แก้ไขช่องโหว่ CVE-2024-12797 ป้องกันการโจมตีแบบ Man-in-the-Middle

OpenSSL ได้ออกแพตช์แก้ไขช่องโหว่ที่มีความรุนแรงสูง ที่หมายเลข CVE-2024-12797 ซึ่งถูกค้นพบโดย Apple และถูกใช้โจมตีแบบ Man-in-the-Middle (MitM) ช่องโหว่นี้ส่งผลกระทบต่อ TLS/DTLS clients ที่เปิดใช้ Raw Public Keys (RPKs) ตามมาตรฐาน RFC7250 และใช้โหมด SSL_VERIFY_PEER โดยมีข้อผิดพลาดในการตรวจสอบความถูกต้องของเซิร์ฟเวอร์ ทำให้แฮกเกอร์สามารถปลอมแปลงและดักฟังข้อมูลได้

ช่องโหว่นี้กระทบ OpenSSL 3.4, 3.3, 3.2 อย่างไรก็ตาม ค่าเริ่มต้นของ OpenSSLจะปิดใช้งาน RPKs ทำให้มีผลเฉพาะกับผู้ที่เปิดใช้งาน RPKs โดยเจาะจง OpenSSL ได้ออกแพตช์เวอร์ชัน 3.4.1, 3.3.2 และ 3.2.4 เพื่อแก้ไขปัญหานี้ ผู้ใช้ที่เปิดใช้ RPKs สามารถตรวจสอบความถูกต้องของการยืนยันตัวตนได้ โดยเรียกใช้ SSL_get_verify_result()

ก่อนหน้านี้ OpenSSL เคยพบช่องโหว่ร้ายแรงอีกสองรายการในปี 2565 ได้แก่ CVE-2022-3602 และ CVE-2022-3786 ซึ่งเป็นปัญหา Buffer Overflow ที่เปิดช่องให้โจมตีผ่านการปลอมแปลงอีเมลในใบรับรอง X.509 อาจทำให้เกิด Denial of Service (DoS) หรือ Remote Code Execution (RCE) ได้

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://securityaffairs.com/174111/security/openssl-patched-the-vulnerability-cve-2024-12797.html