แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ OpenSSL (CVE-2026-22795 และ CVE-2026-22796)

วันที่แจ้งเตือน 3 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานช่องโหว่ของผลิตภัณฑ์ OpenSSL โดยเป็นช่องโหว่ความรุนแรงระดับต่ำ จำนวน 2 รายการ ได้แก่

1) CVE-2026-22795: การอ้างอิงตำแหน่งหน่วยความจำที่ผิดพลาด (Invalid or NULL pointer dereference) ในแอปพลิเคชัน ในขณะที่กำลังประมวลผลไฟล์ PKCS#12 ที่มีรูปแบบไม่ถูกต้อง (Malformed) และ

2) CVE-2026-22796: การระบุประเภทข้อมูลผิดพลาด (Type Confusion) ในขั้นตอนการตรวจสอบลายเซ็น (Signature Verification) ของข้อมูล PKCS#7 ที่มีการลงนามไว้ ส่งผลให้เกิดการอ้างอิงตำแหน่งหน่วยความจำที่ผิดพลาด (Invalid or NULL pointer dereference) เมื่อประมวลผลไฟล์ PKCS#7 ที่มีรูปแบบไม่ถูกต้อง)

อย่างไรก็ดีแม้ช่องโหว่ดังกล่าวจะมีความรุนแรงระดับต่ำ แต่หากเซิร์ฟเวอร์หรือเกตเวย์ที่ทำหน้าที่ตรวจสอบลายเซ็นดิจิทัลถูกโจมตีด้วยไฟล์ PKCS#7 อันตรายจำนวนมาก อาจทำให้บริการหยุดชะงัก ส่งผลต่อ SLA และความเชื่อมั่นของบริษัท

ThaiCERT แนะนำให้ผู้ดูแลระบบและผู้ใช้งานผลิตภัณฑ์ ที่ได้รับผลกระทบพิจารณาดำเนินการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต

ผลิตภัณฑ์	เวอร์ชันที่ได้รับผลกระทบ	เวอร์ชันที่แก้ไขแล้ว
OpenSSL 3.6	3.6.0	3.6.1
OpenSSL 3.5	3.5.0 - 3.5.4	3.5.5
OpenSSL 3.4	3.4.0 - 3.4.3	3.4.4
OpenSSL 3.3	3.3.0 - 3.3.5	3.3.6
OpenSSL 3.0	3.0.0 - 3.0.18	3.0.19
OpenSSL 1.1.1	1.1.1 (All)	1.1.1ze
OpenSSL 1.0.2	1.0.2 (All) *(ไม่ได้รับผลกระทบจาก CVE-2026-22795)*	1.0.2zn

* PKCS (Public Key Cryptography Standards) เป็นมาตรฐานที่ประกาศโดยบริษัท RSA Security Inc. สำหรับการเข้ารหัสลับด้วยเทคโนโลยี เช่น RSA Algorithm, Schnoor signature Algorithm เป็นต้น ทั้งนี้ ตัวอย่างมาตรฐาน PKCS เช่น PKCS#7 ใช้สำหรับการเข้ารหัสลับข้อความด้วย PKI และ ใช้กับการส่ง certificate, PKCS#12 กำหนด file format สำหรับการจัดเก็บ private key อย่างมั่นคงปลอดภัย เป็นต้น (Ref: https://www.etda.or.th/en/list-search.aspx?searchtext=pkcs)

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 2 ก.พ. 2569
2) https://openssl-library.org/news/secadv/20260127.txt
3) https://nvd.nist.gov/vuln/detail/CVE-2026-22795
4) https://nvd.nist.gov/vuln/detail/CVE-2026-22796