

แจ้งเตือนช่องโหว่ OpenSSL (CVE-2026-84782)

วันที่แจ้งเตือน 8 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานช่องโหว่ในไลบรารี OpenSSL (CVE-2026-84782) โดยผู้ไม่หวังดีอาศัยช่องโหว่ดังกล่าวทำให้โปรแกรมเสียหาย (crash) หยุดทำงาน (Denial of Service) และทำให้ข้อมูลในหน่วยความจำ Heap รั่วไหล นำไปสู่การเปิดเผยข้อมูลสำคัญได้ ดังนี้

ช่องโหว่	ผลกระทบ
- ช่องโหว่ประเภท Out-of-bounds Read เกิดขึ้นในกระบวนการ DTLS (Datagram Transport Layer Security) Handshake Retransmission - โปรโตคอล DTLS ใช้สำหรับรักษาความปลอดภัยในการรับส่งข้อมูล โดยหากกระบวนการ Handshake ขนาดใหญ่ ถูกพักการส่งไว้ชั่วคราวเนื่องจาก Buffer เต็ม หรือ Connection ไม่สามารถรับข้อมูลเพิ่มเติมได้ ในขณะนั้นกลไก Retransmission Timer ซึ่งทำหน้าที่ส่งข้อความ Handshake ซ้ำ อาจพยายามส่งข้อความ Handshake ก่อนหน้าอีกครั้ง โดยอ้างอิงตำแหน่งข้อมูลภายใน Buffer ที่ไม่ถูกต้อง ส่งผลให้เกิดการอ่านข้อมูลเกินขอบเขตของ Buffer - หากการอ่านข้อมูลดังกล่าวเข้าถึงพื้นที่หน่วยความจำที่ไม่ได้ถูก Map ไว้ อาจส่งผลให้ระบบหยุดทำงาน และทำให้ระบบไม่พร้อมใช้งาน (Denial of Service: DoS) นอกจากนี้ ข้อมูลจากหน่วยความจำอาจถูกส่งออกไปในรูปแบบข้อความ Handshake ที่ไม่ได้เข้ารหัส ซึ่งอาจส่งผลให้เกิดการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ (Information Disclosure)	ระบบที่ได้รับผลกระทบ - OpenSSL เวอร์ชัน 4.0.0 ถึงก่อนเวอร์ชัน 4.0.3 - OpenSSL เวอร์ชัน 3.6.0 ถึงก่อนเวอร์ชัน 3.6.5 - OpenSSL เวอร์ชัน 3.5.0 ถึงก่อนเวอร์ชัน 3.5.9 - OpenSSL เวอร์ชัน 3.4.0 ถึงก่อนเวอร์ชัน 3.4.8 - OpenSSL เวอร์ชัน 3.0.0 ถึงก่อนเวอร์ชัน 3.0.23 - OpenSSL เวอร์ชัน 1.1.1 ถึงก่อนเวอร์ชัน 1.1.1zj - OpenSSL เวอร์ชัน 1.0.2 ถึงก่อนเวอร์ชัน 1.0.2zs
แนวทางป้องกัน: - อัปเดต OpenSSL เป็นเวอร์ชันที่แก้ไขช่องโหว่ทันที: 4.0.3, 3.6.5, 3.5.9 หรือ 3.4.8 - สำหรับผู้ใช้ Ubuntu ให้ติดตั้งแพตช์ล่าสุด ได้แก่ - Ubuntu 26.04 LTS (libssl3t64 3.5.5-1ubuntu3.6) - Ubuntu 24.04 LTS (libssl3t64 3.0.13-0ubuntu3.16) - Ubuntu 22.04 LTS (libssl3 3.0.2-0ubuntu1.30) - สำหรับผู้ใช้ Debian 13 ให้ติดตั้งแพตช์ OpenSSL เวอร์ชัน 3.5.7-1~deb13u3 (DSA-6531-1) - สำหรับผู้ใช้ OpenSSL 3.0 ที่ไม่สามารถอัปเดตเป็นเวอร์ชันใหม่ได้ ให้พิจารณาซื้อสัญญา Premium Support จาก OpenSSL เพื่อรับแพตช์ 3.0.23 หรือพิจารณาอัปเกรดเป็น OpenSSL 3.5 (LTS) หรือ 4.0 - ตรวจสอบว่าซอฟต์แวร์ภายในองค์กรมีการใช้งาน OpenSSL สำหรับโปรโตคอล DTLS หรือไม่โดยเฉพาะระบบ WebRTC และระบบโทรศัพท์ผ่านอินเทอร์เน็ต (VoIP)	

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 8 ต.ค. 2569

2. <https://openssl-library.org/news/vulnerabilities/index.html?#CVE-2026-84782>

3. <https://thehackernews.com/2026/09/openssl-fixes-high-severity-dtls-flaw.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ