แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ในไลบรารี libssh2

วันที่แจ้งเตือน 8 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ กรณีช่องโหว่ใน libssh2 เสี่ยงถูกรันโค้ดอันตราย บนเครื่อง Client ผ่าน SSH Server โดยมีรายละเอียดดังนี้

การโจมตี	ผลิตภัณฑ์หรือระบบที่อาจได้รับผลกระทบ
ช่องโหว่ CVE-2026-55200 เป็นช่องโหว่ที่เกิดจากการตรวจสอบค่า packet_length ในฟังก์ชัน ssh2_transport_read () ในไลบรารี libssh2 ไม่เพียงพอ ซึ่งผู้ไม่หวังดีสามารถใช้ประโยชน์โดยส่ง SSH Packet ที่มีขนาดไม่ตรงตามมาตรฐานกำหนด เพื่อทำให้เกิดความผิดพลาดด้านหน่วยความจำประเภท Out-of-Bounds Write หรือ Integer Overflow to Buffer Overflow โดยผู้พัฒนา libssh2 ได้ออกแพตช์เพื่อแก้ไขแล้ว ทั้งนี้ libssh2 ถูกใช้งานในซอฟต์แวร์หลายประเภท เช่น เครื่องมือโอนถ่ายไฟล์ เครื่องมือสำหรับนักพัฒนา ระบบสำรองข้อมูล โปรแกรมที่เกี่ยวข้องกับ Git, CURL และ PHP รวมถึงอุปกรณ์หรือระบบที่มี libssh2 เป็นส่วนประกอบ เป็นต้น จึงอาจมีความเสี่ยงแม้ผู้ดูแลระบบ ไม่ได้ติดตั้ง libssh2 โดยตรง **ผู้ไม่หวังดีส่ง Packet ปลอมที่ระบุขนาดข้อมูลใหญ่เกินจริง –> libssh2 ตรวจสอบไม่เพียงพอ –> ข้อมูลล้นหน่วยความจำ –> ระบบล่ม/ถูกยึดเครื่อง**	• ระบบหรือซอฟต์แวร์ที่ใช้งาน libssh2 เวอร์ชัน 1.11.1 และก่อนหน้า • โปรแกรมหรือเครื่องมือที่เชื่อมต่อออกไปยัง SSH Server โดยอาศัย libssh2 เป็นส่วนประกอบ • ระบบที่มี libssh2 เป็นส่วนประกอบ เช่น โปรแกรมสำหรับนักพัฒนา ระบบสำรองข้อมูลเครื่องมืออัปเดตเฟิร์มแวร์ หรือซอฟต์แวร์ที่ถูก build แบบ static linking เป็นต้น • องค์กรที่มีระบบ Client เชื่อมต่อไปยัง SSH Server ภายนอก ที่ไม่สามารถยืนยันความน่าเชื่อถือได้ **หากเครื่อง Client ที่ได้รับผลกระทบมีสิทธิ์เข้าถึงระบบสำคัญ อาจถูกใช้เป็นจุดเริ่มต้นในการโจมตีต่อเนื่องภายในองค์กร**

แนวทางการป้องกันและลดความเสี่ยง

- ตรวจสอบซอฟต์แวร์ ระบบ หรืออุปกรณ์ที่ใช้งาน libssh2 โดยเฉพาะเวอร์ชัน 1.11.1 และก่อนหน้า
- ติดตั้งแพตช์หรือแพ็กเกจที่มีการแก้ไข ตามประกาศจากผู้พัฒนา ระบบปฏิบัติการ หรือผู้จำหน่ายซอฟต์แวร์ที่เกี่ยวข้อง
- ตรวจสอบซอฟต์แวร์หรือระบบที่มี libssh2 เป็นส่วนประกอบ เนื่องจากการอัปเดตแพ็กเกจของระบบปฏิบัติการอาจไม่ครอบคลุม
- ระหว่างรอการอัปเดต ควรจำกัดการเชื่อมต่อ SSH ออกไปยัง Server ที่เชื่อถือได้เท่านั้น และตรวจสอบ SSH Host Key ของปลายทางก่อนเชื่อมต่อ
- เฝ้าระวังเหตุการณ์ผิดปกติ เช่น โปรแกรม Client ขัดข้องหลังเชื่อมต่อ SSH, การเชื่อมต่อ SSH ไปยังปลายทางที่ไม่น่าเชื่อถือ หรือพฤติกรรมหน่วยความจำผิดปกติบนระบบที่ใช้ libssh2

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 7 ก.ค. 2569
2. https://www.vulncheck.com/advisories/libssh2-out-of-bounds-write-via-unchecked-packet-length-in-transport-c
3. https://thehackernews.com/2026/06/public-poc-released-for-critical.html?