แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ร้ายแรง React2Shell (CVE-2025-55182) ถูกนำไปใช้โจมตีระบบ

วันที่แจ้งเตือน 8 ธันวาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารพบว่า กลุ่มผู้ไม่ประสงค์ดีได้นำช่องโหว่ระดับร้ายแรง React2Shell (CVE-2025-55182) ซึ่งเพิ่งถูกเปิดเผยสู่สาธารณะ ไปใช้โจมตีระบบขององค์กรในหลายภูมิภาค

ช่องโหว่ดังกล่าวเกิดจากข้อบกพร่องในการประมวลผลข้อมูล (payload) ที่ถูกส่งไปยัง React Server Function endpoints ทำให้ผู้ไม่ประสงค์ดีสามารถส่งคำขอ HTTP ที่ถูกปรับแต่ง เพื่อบังคับให้ระบบทำการ deserialization และรันคำสั่ง JavaScript บนเซิร์ฟเวอร์ได้โดยไม่ต้องผ่านการยืนยันตัวตน แม้ระบบไม่ได้ใช้งาน Server Function โดยตรง แต่หากมีการรองรับ React Server Components จะยังคงมีความเสี่ยงที่จะได้รับผลกระทบ โดยแพ็กเกจ npm ที่พบว่ามีช่องโหว่นี้ ได้แก่ (1) react-server-dom-webpack (2) react-server-dom-parcel และ (3) react-server-dom-turbopack ซึ่งผู้พัฒนาได้ออกเวอร์ชันแก้ไขแล้วในรุ่น 19.0.1, 19.1.2 และ 19.2.1

นอกจากนี้ ช่องโหว่นี้ยังส่งผลกระทบต่อ Next.js (App Router) ภายใต้รหัสช่องโหว่ CVE-2025-66478 โดยเวอร์ชันที่มีความเสี่ยงประกอบด้วย ≥14.3.0-canary.77, ≥15 และ ≥16 ซึ่งได้รับการแก้ไขแล้วในรุ่น 16.0.7, 15.5.7, 15.4.8, 15.3.6, 15.2.6, 15.1.9 และ 15.0.5 รวมถึง libraries อื่นที่มีการ bundle RSC เช่น Vite RSC plugin, Parcel RSC plugin, React Router RSC preview, RedwoodJS และ Waku ที่อาจได้รับผลกระทบเช่นกัน ผู้ประกอบธุรกิจจึงควรตรวจสอบสภาพแวดล้อมระบบงานที่ใช้งาน React RSC และดำเนินการอัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันที่ปลอดภัยโดยเร็ว เพื่อลดความเสี่ยงจากการถูกโจมตีในลักษณะดังกล่าว

ผู้ประกอบธุรกิจและผู้ดูแลระบบ ควรพิจารณาดำเนินมาตรการป้องกันความเสี่ยงและภัยคุกคามจากช่องโหว่ดังกล่าว โดยดำเนินการอัปเดต React Server Components ให้เป็นเวอร์ชันที่ได้รับการแก้ไขแล้ว พร้อมทั้งตรวจสอบระบบงานที่ใช้งาน React RSC และบริการที่เชื่อมต่ออยู่ทั้งหมด โดยเฉพาะระบบ Web Application ที่ใช้ RSC ในการประมวลผล นอกจากนี้ควรทบทวนบันทึกเหตุการณ์ย้อนหลัง ตรวจสอบการเข้าถึงของบัญชีผู้ใช้งานและการดำเนินการกรณีที่มีความผิดปกติ เพื่อลดโอกาสและผลกระทบที่อาจทำให้เกิดความเสี่ยงต่อหน่วยงาน

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

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2025-55182
2. https://thehackernews.com/2025/12/critical-rsc-bugs-in-react-and-nextjs.html

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ