แจ้งเตือน

Critical

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

แจ้งเตือน ช่องโหว่ Zero Day ใน PostgreSQL (CVE-2025-1094)

วันที่แจ้งเตือน 19 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ และพบการรายงานช่องโหว่ Zero Day (CVE-2025-1094) ใน PostgreSQL ที่ส่งผลต่อความมั่นคงปลอดภัยของระบบฐานข้อมูล ช่องโหว่ดังกล่าวมีสาเหตุมาจาก PostgreSQL ประมวลผลข้อมูลนำเข้าผิดพลาด เช่น ชุดอักขระ UTF-8 ที่ไม่ถูกต้อง เป็นต้น ซึ่งอาจถูกใช้โจมตีแบบ SQL Injection ผ่านเครื่องมือ PostgreSQL Interactive Tool (PSQL) เพื่อเข้าถึงและแก้ไขข้อมูลในฐานข้อมูล อีกทั้งสามารถเรียกใช้โค้ดระยะไกล หรือ Remote Code Execution (RCE) บนเครื่อง Server ที่มีช่องโหว่ได้

นักวิจัยด้านความมั่นคงปลอดภัยจาก Rapid7 แนะนำให้ผู้ใช้งานระบบฐานข้อมูล PostgreSQL เวอร์ชั่นก่อนหน้า ทำการอัปเดตเป็นเวอร์ชันล่าสุด ซึ่งได้รับการแก้ไขช่องโหว่แล้ว ได้แก่ เวอร์ชัน 17.3, 16.7, 15.11, 14.16 และ 13.19

สำหรับผู้ประกอบธุรกิจที่ใช้ระบบฐานข้อมูล PostgreSQL ควรพิจารณาดำเนินการอัปเดตเวอร์ชันของระบบฐานข้อมูลดังกล่าว ตรวจสอบและทบทวนมาตรการควบคุมการเข้าถึง เพื่อให้มีประสิทธิภาพอยู่เสมอ ติดตามและวิเคราะห์บันทึกการใช้งาน (Log) ทดสอบการสำรองข้อมูล เพื่อให้มั่นใจว่าข้อมูลดังกล่าวสามารถนำมาใช้งานได้ เมื่อมีเหตุจำเป็นและให้ความสำคัญในการพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยให้พร้อมรับมือกับภัยคุกคามรูปแบบใหม่ รวมทั้ง ติดตามข่าวสารและประกาศเตือนภัยเกี่ยวกับช่องโหว่ต่าง ๆ อย่างใกล้ชิดจะช่วยให้องค์กรสามารถปรับตัวและตอบสนองต่อความเสี่ยงได้อย่างเหมาะสม

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/postgresql-flaw-exploited-as-zero-day-in-beyondtrust-breach/
2. https://thehackernews.com/2025/02/postgresql-vulnerability-exploited.html
3. https://www.postgresql.org/support/security/CVE-2025-1094/