วันที่ 7 กันยายน 2569

ช่องโหว่ PostgreSQL อายุ 12 ปี เปิดทางให้ยึดฐานข้อมูลและเซิร์ฟเวอร์ได้

PostgreSQL รุ่นที่เผยแพร่ตั้งแต่ปี 2014 เป็นต้นมามีช่องโหว่ร้ายแรงที่เปิดทางให้ผู้โจมตีซึ่งมีสิทธิ์ในระดับต่ำ สามารถเข้าควบคุมฐานข้อมูลและเซิร์ฟเวอร์ได้ ตามรายงานของบริษัทด้านความปลอดภัยทางไซเบอร์ Cyera

PostgreSQL เป็นระบบจัดการฐานข้อมูลเชิงสัมพันธ์แบบโอเพนซอร์สที่รองรับทั้งการค้นหาข้อมูลแบบเชิงสัมพันธ์ (SQL) และแบบไม่ใช่เชิงสัมพันธ์ (JSON) และเป็นหนึ่งในระบบฐานข้อมูลที่ได้รับความนิยมมากที่สุด โดยมีบริษัทหลายหมื่นแห่ง รวมถึงองค์กรขนาดใหญ่นำไปใช้งาน ช่องโหว่นี้ถูกติดตามในชื่อ CVE-2026-6471 (คะแนน CVSS 7.2) และถูกเรียกว่า PostGREShell โดยช่องโหว่ดังกล่าวสามารถถูกใช้เพื่อรันโค้ดจากระยะไกล (Remote Code Execution) และยกระดับสิทธิ์ (Privilege Escalation) ได้

ช่องโหว่นี้เกิดจากการขาดการตรวจสอบสิทธิ์ในระบบ Logical Decoding ของฐานข้อมูล และสามารถถูกโจมตีได้โดยผู้โจมตีที่มีสิทธิ์ Replication ซึ่งทำให้สามารถโหลดไฟล์ใดๆ ที่ระบบปฏิบัติการอนุญาตให้บัญชีที่ใช้รันเซิร์ฟเวอร์เข้าถึงได้ ผ่าน Logical Decoding Plugin

Cyera อธิบายว่า PostgreSQL ใช้โปรโตคอลเฉพาะสำหรับการทำ Replication เพื่อซิงค์ฐานข้อมูลจากเซิร์ฟเวอร์หลักไปยังเซิร์ฟเวอร์สำรองหลายตัว ซึ่งใช้สำหรับการสำรองข้อมูลและการกู้คืนระบบ โดยบัญชีที่มีคุณสมบัติ Replication จะต้องถูกใช้สำหรับกระบวนการดังกล่าว และมักมีการมอบสิทธิ์นี้ให้กับเครื่องมือสำรองข้อมูล เซิร์ฟเวอร์ Pipeline และระบบ Monitoring ที่เชื่อมต่อเข้ามา การเปลี่ยนแปลงต่างๆ จะถูกบันทึกไว้ในระบบ Local Replication ในรูปแบบเหตุการณ์ของตาราง เพื่อให้เครื่องมือภายนอกสามารถอ่านข้อมูลเหล่านี้ได้ โดยเครื่องมือดังกล่าวจะสร้าง Logical Replication Slot และระบุชื่อ Output Plugin ที่ PostgreSQL จะโหลดขึ้นมาเพื่อจัดรูปแบบข้อมูลที่ส่งออก

เมื่อมีการโหลด Plugin PostgreSQL จะเรียกใช้ฟังก์ชันเริ่มต้นของ Plugin ด้วยสิทธิ์เดียวกับที่ใช้รันเซิร์ฟเวอร์ เพื่อป้องกันการนำระบบไปใช้ในทางที่ผิด ผู้ใช้ที่ไม่ใช่ Superuser จึงสามารถโหลด Plugin ได้เฉพาะจากไดเรกทอรีที่ผู้ดูแลระบบเป็นผู้ควบคุมเท่านั้น

Cyera พบว่าชื่อของ Plugin ถูกส่งต่อไปยังตัว Loader โดยตรง โดยไม่มีการตรวจสอบหรือทำความสะอาดข้อมูล ทำให้ผู้โจมตีสามารถระบุเส้นทางไฟล์แบบเต็มบนระบบให้ Loader โหลดได้ และไฟล์ดังกล่าวจะถูกส่งให้กับ dlopen() ซึ่งเป็นฟังก์ชันของ C/C++ ที่ใช้สำหรับโหลด Shared Library แบบไดนามิก

ตัว Parser ของโปรโตคอล Replication ยอมรับอักขระแทบทุกชนิดภายในชื่อ Plugin ที่อยู่ในเครื่องหมายคำพูดคู่: ทั้ง Slash, Backslash, จุด, การใช้ ../ เพื่อย้อนกลับไปยังไดเรกทอรีก่อนหน้า รวมถึง Windows UNC Path ทำให้ผู้โจมตีสามารถโหลดและสั่งให้ไฟล์ใดๆ ทำงานผ่าน dlopen() ได้ โดยไฟล์ดังกล่าวจะทำงานด้วยสิทธิ์ของบัญชีระบบ postgres โค้ดที่ถูกโหลดผ่าน dlopen() จะทำงานอยู่ใน Address Space เดียวกับ PostgreSQL โดยไม่มี Sandbox และไม่มีการตรวจสอบการเรียกใช้ Internal API เซิร์ฟเวอร์จะเชื่อถือโค้ดที่ถูกโหลดเข้ามาทันที จากนั้น Plugin จะเรียกใช้ฟังก์ชันภายในเพื่อเปลี่ยนตัวเองให้เป็น Bootstrap Superuser ของ Session และเขียนข้อมูลโดยตรงลงใน pg_authid ซึ่งเป็น Catalog Table ที่ใช้กำหนดว่าใครมีสิทธิ์เป็น Superuser จากนั้นจะเปลี่ยนค่า Privilege Flag ทั้งหมดให้เป็น true เมื่อถึงจุดนี้ ผู้โจมตีจะได้รับสิทธิ์ Superuser อย่างถาวร ซึ่งทำให้สามารถเข้าถึงทุกตารางในทุกฐานข้อมูล รันคำสั่งบนระบบปฏิบัติการ อ่าน Private Key และเขียนไฟล์ไปยังตำแหน่งใดๆ ที่ Process ของ postgres มีสิทธิ์เข้าถึงได้

ตามข้อมูลของ Cyera Plugin ดังกล่าวยังสามารถติดตั้งกลไก Backdoor เพื่อคงสิทธิ์การเข้าถึงระบบไว้ได้ เช่น เปิดให้สามารถเชื่อมต่อเข้ามาโดยไม่ต้องใช้รหัสผ่าน คัดลอกตัวเองไปไว้ในตำแหน่งถาวร และลงทะเบียนให้ถูกโหลดซ้ำในทุก Backend ที่เริ่มทำงานใหม่ รวมถึงสามารถนำสิทธิ์ Superuser กลับมาใช้งานอีกครั้งได้ แม้ว่าผู้ดูแลระบบจะพยายามย้อนการเปลี่ยนแปลงแล้วก็ตาม

PostGREShell เปลี่ยน Credential สำหรับ Replication ที่แทบไม่มีใครให้ความสนใจ ให้กลายเป็นช่องทางสำหรับการรันโค้ด การได้รับสิทธิ์ Superuser และการติดตั้ง Backdoor เพื่อคงอยู่ในระบบของฐานข้อมูลที่อยู่เบื้องหลังบริการจำนวนมากบนอินเทอร์เน็ต PostgreSQL ทุกเวอร์ชันตั้งแต่ 9.4 ถึง 18 ได้รับผลกระทบ (เรายืนยันการโจมตีบนเวอร์ชัน 18.2 แล้ว) และเนื่องจาก Logical Replication กลายเป็นส่วนหนึ่งของระบบ Production ที่ใช้งานกันทั่วไป ช่องโหว่นี้จึงมีโอกาสอยู่ในระบบ PostgreSQL แทบทุกแห่ง Cyera ระบุ

CVE-2026-6471 ได้รับการแก้ไขแล้วใน PostgreSQL เวอร์ชัน 18.6, 17.11, 16.15, 15.19 และ 14.24 โดยองค์กรต่างๆ ควรอัปเดต PostgreSQL ที่ใช้งานอยู่โดยเร็วที่สุด ตรวจสอบบัญชีที่มีสิทธิ์ Replication และนำคุณสมบัติ Replication ออกจากบัญชีใดๆ ที่ไม่มีความจำเป็นต้องใช้งาน

ข้อมูลอ้างอิง

Sep 4, 2026, By Ionut Arghire

- https://www.securityweek.com/12-year-old-postgresql-vulnerability-enables-database-server-takeover/