เอกสารแจ้งเตือนกรณีพบช่องโหว่ใน MongoDB Server เสี่ยงถูกเข้าถึงระบบฐานข้อมูลโดยไม่ได้รับอนุญาต

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์กรณีพบช่องโหว่ใน MongoDB Server เสี่ยงถูกเข้าถึงระบบฐานข้อมูลโดยไม่ได้รับอนุญาต นั้น

พบการแจ้งเตือนช่องโหว่ในระบบฐานข้อมูล MongoDB Server ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงสิทธิ์ระดับผู้ดูแลระบบได้โดยไม่ต้องผ่านการยืนยันตัวตน ทำให้ผู้โจมตีอาจเข้าควบคุมระบบเป้าหมาย ติดตั้งมัลแวร์ หรือขโมยข้อมูลสำคัญออกไปได้ โดยผู้ที่ได้รับผลกระทบคือหน่วยงานและองค์กรที่ใช้งาน MongoDB Server เวอร์ชัน 7.0, 8.0 และ 8.3 ที่ยังไม่ได้ทำการอัปเดตแพตช์รักษาความปลอดภัยให้เป็นปัจจุบัน[1]

<u>รายละเอียดช่องโหว่</u>

CVE-2026-82067 (คะแนน CVSSv4.0: 9.2) ช่องโหว่นี้เกิดจากการทำงานผิดพลาดของส่วนตรวจสอบการตั้งค่า (Configuration Validation Component) ภายใน MongoDB Server ส่งผลให้ระบบยืนยันตัวตน (Authorization Subsystem) อาจถูกปิดใช้งานไปโดยไม่ได้ตั้งใจในระหว่างกระบวนการเริ่มต้นระบบ (Server Startup)[2]

<u>ผลกระทบที่อาจเกิดขึ้น</u>

- ยกระดับสิทธิ์จากผู้ใช้งานทั่วไปเป็นผู้ดูแลระบบ
- ควบคุมการทำงานของเครื่องเป้าหมาย
- ติดตั้งซอฟต์แวร์หรือมัลแวร์เพิ่มเติม รวมถึงการเข้าถึงหรือแก้ไขข้อมูลภายในระบบ

<u>ผลิตภัณฑ์ที่ได้รับผลกระทบ</u>

- MongoDB Server 7.0 ต่ำกว่า 7.0.41
- MongoDB Server 8.0 ต่ำกว่า 8.0.30
- MongoDB Server 8.3 ต่ำกว่า 8.3.9

<u>แนวทางการแก้ไขและป้องกัน</u>

- อัปเดต MongoDB Server เวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้วโดยเร็ว
- ตรวจสอบการตั้งค่าความปลอดภัยของฐานข้อมูล เช่น ตรวจสอบว่าเปิดใช้งานการยืนยันตัวตน (Authentication) อยู่หรือไม่ ตรวจสอบสิทธิ์ของบัญชีผู้ใช้งาน จำกัดการเข้าถึง MongoDB เฉพาะระบบหรือเครือข่ายที่จำเป็น เป็นต้น
- หากพบว่า MongoDB Server มีความเสี่ยง ดำเนินการตรวจสอบเหตุการณ์ในทันที เช่น การสร้างบัญชีผู้ดูแลระบบที่ไม่ได้รับอนุญาต การเปลี่ยนแปลงสิทธิ์ผู้ใช้งาน การส่งออกข้อมูล (Data Exfiltration)

ทั้งนี้หน่วยงานสามารถตรวจสอบข้อมูลเพิ่มเติมได้ที่ https://dg.th/pjlc23eixd และ https://dg.th/k9xjhserc6

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบตรวจสอบเวอร์ชันของผลิตภัณฑ์ รวมทั้งดำเนินการอัปเดต MongoDB Server ให้เป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้วโดยเร็ว เพื่อป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ นอกจากนี้ควรเฝ้าระวังกิจกรรมที่ผิดปกติหรือพฤติกรรมที่อาจบ่งชี้ถึงการถูกโจมตีหรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการที่สำคัญอย่างต่อเนื่อง ทั้งนี้ สามารถติดตามข่าวสารและคำแนะนำด้านภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://dg.th/brsu85qwdc
2. https://dg.th/6412wcdn3g