วันที่ 16 ตุลาคม 2568

ช่องโหว่ใหม่ใน Oracle E-Business Suite อาจเปิดทางให้แฮ็กเกอร์เข้าถึงข้อมูลได้โดยไม่ต้องล็อกอิน

Oracle ได้ออกประกาศแจ้งเตือนด้านความปลอดภัยเมื่อวันเสาร์ที่ผ่านมาเกี่ยวกับช่องโหว่ใหม่ล่าสุดที่ส่งผลกระทบต่อระบบ Oracle E-Business Suite (EBS) โดยช่องโหว่นี้อาจทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลสำคัญได้โดยไม่ได้รับอนุญาต

รายละเอียดทางเทคนิคของช่องโหว่ใหม่

ช่องโหว่นี้ถูกระบุภายใต้รหัส CVE-2025-61884 โดยมีคะแนนความรุนแรง CVSS อยู่ที่ 7.5 ซึ่งถือว่าอยู่ในระดับสูง ช่องโหว่นี้ส่งผลกระทบต่อระบบ EBS เวอร์ชัน 12.2.3 ถึง 12.2.14

กลไกการโจมตี (ตามฐานข้อมูล NIST - NVD):

- เงื่อนไขการโจมตี: “ช่องโหว่นี้สามารถถูกโจมตีได้ง่าย โดยผู้โจมตีที่ไม่มีบัญชีผู้ใช้ (unauthenticated) สามารถเข้าถึงระบบผ่านเครือข่าย HTTP เพื่อเจาะระบบ Oracle Configurator ได้สำเร็จ”
- ผลกระทบ: “หากการโจมตีสำเร็จอาจทำให้ผู้ไม่หวังดีเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต หรือเข้าถึงข้อมูลทั้งหมดที่อยู่ใน Oracle Configurator ได้อย่างเต็มรูปแบบ”

Rob Duhart หัวหน้าฝ่ายความปลอดภัยของ Oracle กล่าวเพิ่มเติมว่าช่องโหว่นี้ส่งผลต่อ “บางการติดตั้ง” ของระบบ E-Business Suite และอาจถูกนำไปใช้เพื่อเข้าถึงทรัพยากรที่มีข้อมูลสำคัญได้

Oracle ย้ำในประกาศแยกต่างหากว่าช่องโหว่นี้สามารถถูกโจมตีจากระยะไกลได้โดย ไม่จำเป็นต้องล็อกอินเข้าสู่ระบบ ซึ่งทำให้การอัปเดตแพตช์กลายเป็นสิ่งจำเป็นอย่างเร่งด่วน อย่างไรก็ตามขณะนี้ยังไม่มีรายงานว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริงในโลกออนไลน์

เหตุการณ์ต่อเนื่อง: ต้องระวังการโจมตีแบบ Zero-day ซ้ำซ้อน

การแจ้งเตือนช่องโหว่ใหม่นี้เกิดขึ้นไม่นานหลังจากที่ทีม Google Threat Intelligence Group (GTIG) และบริษัท Mandiant เพิ่งเปิดเผยรายงานการโจมตีแบบ zero-day ในวงกว้างก่อนหน้านี้

การโจมตีระลอกก่อนหน้านี้ใช้ช่องโหว่ CVE-2025-61882 ในซอฟต์แวร์ Oracle E-Business Suite (EBS) ซึ่งถูกพบว่ามีความร้ายแรงสูงกว่า (CVSS: 9.8) โดยผู้โจมตีใช้ช่องโหว่นี้เพื่อเรียกใช้ payload สองรูปแบบ ซึ่งนำไปสู่การติดตั้งมัลแวร์หลายตระกูล เช่น GOLDVEIN.JAVA, SAGEGIFT, SAGELEAF และ SAGEWAVE

แม้ว่า Oracle จะยังไม่ได้ระบุชื่อกลุ่มแฮ็กเกอร์ที่อยู่เบื้องหลังการโจมตีครั้งก่อนอย่างเป็นทางการ แต่มีความเชื่อว่ากลุ่มผู้โจมตีมีความเชื่อมโยงกับกลุ่มแรนซัมแวร์ Cl0p

องค์กรที่ใช้งาน Oracle E-Business Suite เวอร์ชันที่ได้รับผลกระทบ (12.2.3 ถึง 12.2.14) ควรอัปเดตแพตช์สำหรับช่องโหว่ CVE-2025-61884 ทันที เพื่อป้องกันความเสี่ยงในการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต เนื่องจากช่องโหว่นี้สามารถถูกโจมตีจากระยะไกลได้โดยไม่ต้องล็อกอินเข้าสู่ระบบ

ข้อมูลอ้างอิง

Oct 12, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/new-oracle-e-business-suite-bug-could.html