แจ้งเตือน

Alert

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

กลุ่ม ShinyHunters โจมตีผ่านช่องโหว่ Zero-Day ใน Oracle PeopleSoft (CVE-2026-35273)

วันที่แจ้งเตือน 6 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานกรณี Nissan Americas ได้เปิดเผยเหตุการณ์ข้อมูลรั่วไหลที่ส่งผลกระทบต่อพนักงานปัจจุบันและอดีตพนักงาน หลังได้รับแจ้งว่าผู้โจมตีได้ใช้ประโยชน์จากช่องโหว่ Zero-day ใน Oracle PeopleSoft (CVE-2026-35273)

Oracle PeopleSoft เป็นซอฟต์แวร์สำหรับบริหารจัดการข้อมูลพนักงาน มีหลายฟังก์ชัน เช่น ระบบเงินเดือน การบริหารภาษี เป็นต้น ซึ่งข้อมูลที่ได้รับผลกระทบ ได้แก่ ข้อมูลการติดต่อ ข้อมูลบัญชีธนาคาร หมายเลขประจำตัวประชาชน ข้อมูลทางการเงิน ภาษี และผู้รับผลประโยชน์ โดยกลุ่ม ShinyHunters ระบุว่าสามารถเจาะระบบ Oracle PeopleSoft ได้กว่า 300 ระบบ

ทั้งนี้ ShinyHunters เป็นกลุ่มอาชญากรไซเบอร์ ที่มักจะก่ออาชญากรรมด้วยการข่มขู่เรียกค่าไถ่ โดยมุ่งโจมตีระบบงานที่ทำงานบนบริการคลาวด์ และ Software-as-a-Service (SaaS) รวมถึงผู้ใช้บริการเชื่อมต่อระบบของบุคคลที่ 3 (3rd Party) เพื่อขโมยข้อมูลองค์กร และไม่ได้ใช้มัลแวร์ที่ซับซ้อนเพื่อเข้าไปล็อคไฟล์ แต่จะเน้นการขโมยหรือก๊อปปี้ข้อมูลออกไปก่อน จากนั้นจึงนำข้อมูลนั้นมาเป็นตัวประกันเพื่อขู่กรรโชกทรัพย์ (Data Extortion) โดยขู่ว่าถ้ายอมไม่จ่ายเงิน จะนำข้อมูลไปขายหรือปล่อยหลุดสู่สาธารณะ

การโจมตีของ ShinyHunters นั้น ระบบขององค์กรเป้าหมายยังสามารถทำงานได้ตามปกติโดยไม่รู้ว่าถูกโจมตี แต่ในความเป็นจริงข้อมูลสำคัญของลูกค้า พนักงาน หรือธุรกิจได้ถูกดึงออกไปและพร้อมจะถูกนำไปขายแล้ว โดยพุ่งเป้าไปที่ระบบ SaaS ที่นิยมใช้เก็บข้อมูล เช่น Snowflake, Salesforce หรือ Canvas LMS โดยมักอาศัย Credential (รหัสผ่าน) หรือการตั้งค่าระบบ (Configuration) ที่อ่อนแอ รวมถึงใช้เทคนิค Social Engineering และ Vishing เพื่อหลอกให้ผู้ใช้งานในองค์กรเป้าหมายเชื่อมต่อเครื่องมือเข้ากับระบบและเปิดทางให้ผู้ไม่หวังดีดึงข้อมูลออกไปได้

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำหรับผู้ประกอบธุรกิจที่มีงานใช้งาน Oracle PeopleSoft ขอให้พิจารณาดำเนินการตรวจสอบการติดตั้งแพตช์หรือมาตรการบรรเทาความเสี่ยงจาก Oracle พร้อมทั้งเฝ้าระวังกิจกรรมที่ผิดปกติ โดยเฉพาะการเข้าถึงระบบ HR และฐานข้อมูลบุคลากร รวมไปถึงทบทวนสิทธิ์การเข้าถึงระบบและใช้การยืนยันตัวตนแบบ MFA สำหรับผู้ดูแลระบบและผู้ใช้งานที่มีสิทธิ์สูง และเตรียมแผน Incident Response และแนวทางแจ้งเหตุข้อมูลรั่วไหลให้พร้อม หากพบว่ามีข้อมูลส่วนบุคคลได้รับผลกระทบ

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2026-35273
2. https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
3. https://www.bleepingcomputer.com/news/security/nissan-discloses-employee-data-breach-linked-to-oracle-zero-day-attacks/