แจ้งเตือน : ช่องโหว่

Critical

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

แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ VMware vCenter Server (CVE-2024-37079, CVE-2024-37080 และ CVE-2024-37081)

วันที่แจ้งเตือน 26 มกราคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงาน ก.ล.ต. ร่วมกับ TCM-CERT ได้ติดตามข่าวเกี่ยวกับการโจมตีทางไซเบอร์ พบรายงานช่องโหว่ร้ายแรงของผลิตภัณฑ์ Vmware จำนวน 3 รายการ ได้แก่ ช่องโหว่ร้ายแรง CVE-2024-37079, CVE-2024-37080 Heap-overflow ในโปรโตคอล DCE/RPC ซึ่งผู้ไม่หวังดีใช้เข้าถึงเครือข่ายของ vCenter Server และส่ง Packet เพื่อสั่งรันโค้ดอันตรายจากระยะไกล (RCE) โดยไม่ต้องยืนยันตัวตน อาจนำไปสู่การยึดครองระบบทั้งหมด รวมถึง CVE-2024-37081 ซึ่งเป็นช่องโหว่ที่ Local user สามารถยกระดับสิทธิ์ตัวเองเป็น Root บน vCenter Server Appliance ได้ ทั้งนี้ Cybersecurity and Infrastructure Security Agency (CISA) ได้เพิ่มช่องโหว่ของผลิตภัณฑ์ Vmware ที่ได้รับการยืนยันว่ามีการใช้งานจริงในการโจมตี (Actively Exploited) เข้าฐานข้อมูล KVE catalog ได้แก่ CVE-2024-37079

ผลิตภัณฑ์ที่ได้รับผลกระทบ ดังนี้

VMware Product	Effected version	Fixed Release (อ้างอิง2)
vCenter Server	affected from 8.0 before 8.0 U2d affected from 8.0 before 8.0 U1e affected from 7.0 before 7.0 U3r	Update to 8.0 U2d Update to 8.0 U1e Update to 7.0 U3r
Cloud Foundation (vCenter Server)	4.x 5.X	Async patch (KB88287)

ทั้งนี้ VMware ได้ออกคำแนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการอัปเดตซอฟตแวร์เปนเวอรชันตามที่ VMware แนะนำโดยเร็วที่สุด

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/01/cisa-adds-actively-exploited-vmware.html
2. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/securityadvisories/0/24453