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 ช่องโหว่ Zero-Days ของผลิตภัณฑ์ VMware (CVE-2025-22224, CVE-2025-22225 และ CVE-2025-22226)

วันที่แจ้งเตือน 6 มีนาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงาน ก.ล.ต. ร่วมกับ TCM-CERT ได้ติดตามข่าวเกี่ยวกับการโจมตีทางไซเบอร์ พบการรายงานช่องโหว่ Zero-days ในผลิตภัณฑ์ Vmware จำนวน 3 รายการ ได้แก่ CVE-2025-22224 (VMCI heap-overflow), CVE-2025-22225 (VMware ESXi arbitrary write) และ CVE-2025-22226 (HGFS information-disclosure) ส่งผลให้ผู้ไม่หวังดีที่ครอบครองสิทธิระดับผู้ดูแลระบบหรือ root สามารถนำช่องโหว่เหล่านี้มาใช้ร่วมกัน เพื่อหลบหนีออกจาก Sandbox ของเครื่อง Virtual Machine และสามารถเข้าถึง Hypervisor ได้ ทั้งนี้ พบว่ามีผู้ไม่หวังดีมีการนำช่องโหว่ดังกล่าวไปใช้ในการโจมตีจริงแล้ว

ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ VMware ESXi, VMware Workstation Pro / Player (Workstation), VMware Fusion, VMware Cloud Foundation และ VMware Telco Cloud Platform ทั้งนี้ VMware ได้ออกคำแนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว ทำการอัปเดตซอฟตแวร์เปนเวอรชันตามที่ VMware แนะนำโดยเร็วที่สุด ดังนี้

VMware Product	Effected version	Fixed Release (อ้างอิง2)
VMware ESXi	7.0 8.0	ESXi70U3s-24585291 ESXi80U2d-24585300 ESXi80U3d-24585383
VMware Workstation	17.x	17.6.3
VMware Fusion	13.x	13.6.3
VMware Cloud Foundation	4.5.x 5.x	Async patch to ESXi70U3s-24585291 Async patch to ESXi80U3d-24585383
VMware Telco Cloud Platform	5.x, 4.x, 3.x, 2.x	KB389385
VMware Telco Cloud Infrastructure	3.x, 2.x	KB389385

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

ข้อมูลอ้างอิง

1) https://www.bleepingcomputer.com/news/security/broadcom-fixes-three-vmware-zero-days-exploited-in-attacks/
2) https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390
3) https://nvd.nist.gov/vuln/detail/CVE-2025-22224
4) https://nvd.nist.gov/vuln/detail/CVE-2025-22225
5) https://nvd.nist.gov/vuln/detail/CVE-2025-22226