TLP:CLEAR

เอกสารการแจ้งเตือนกรณีพบช่องโหว่ในแพลตฟอร์ม VMware vCenter Server

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี VMware ได้ออกอัปเดตเพื่อแก้ไขช่องโหว่จำนวน 2 รายการ ที่ CVE-2024-38812 และ CVE-2024-38813 ที่ส่งผลกระทบต่อ vCenter Server โดยมีรายละเอียดของช่องโหว่ดังต่อไปนี้ [1]

- CVE-2024-38812 คะแนน (CVSSv3 : 9.8) หากมีการใช้ประโยชน์จากช่องโหว่ heap-overflow ได้สำเร็จอาจทำให้ผู้โจมตีสามารถเข้าถึงเครือข่าย และสามารถถูก Remote Code Execution จากระยะไกลได้ โดยการส่งแพ็กเก็ตที่สร้างขึ้นเป็นพิเศษ

- CVE-2024-38813 คะแนน (CVSSv3 : 7.5) หากมีการใช้ประโยชน์จากช่องโหว่ด้วยการ Privilege Escalation ได้สำเร็จ อาจทำให้ผู้โจมตีสามารถเข้าถึงเครือข่าย เพื่อส่งแพ็กเก็ตที่สร้างขึ้นเป็นพิเศษและได้รับสิทธิ์ Root

ช่องโหว่ส่งผลกระทบต่อผลิตภัณฑ์ดังต่อไปนี้

- VMware vCenter Server เวอร์ชัน 7.0 และ 8.0
- VMware Cloud Foundation เวอร์ชัน 4.x และ 5.x [2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบ กิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-119
2. https://www.securityweek.com/vmware-patches-remote-code-execution-flaw-found-in-chinese-hacking-contest/