TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Vmware ได้ออกแก้ไขช่องโหว่ในผลิตภัณฑ์ Workstation และ Fusion desktop hypervisors

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี VMWARE ได้ออกแก้ไขช่องโหว่ในผลิตภัณฑ์ Workstation และ Fusion desktop hypervisors[1] ซึ่งรวมถึงช่องโหว่แบบ Zero-day ที่ส่งผลกระทบต่อ Workstation เวอร์ชัน 17.x และ Fusion เวอร์ชัน 13.x โดยรายละเอียดของช่องโหว่ที่ได้รับการแก้ไขมีดังนี้[2]

– CVE-2024-22267 (CVSS score: 9.3) เป็นช่องโหว่ use-after-free ในอุปกรณ์ Bluetooth ที่ทำให้ผู้ไม่หวังดีมีสิทธิ์เป็นผู้ดูแลระบบใน virtual machine และสามารถใช้ช่องโหว่นี้เพื่อ execute code ในกระบวนการ VMX ของ virtual machine บนโฮสต์ได้

– CVE-2024-22268 (CVSS score: 7.1) เป็นช่องโหว่ประเภท heap buffer-overflow ในฟังก์ชัน Shader ที่ทำให้ผู้ไม่หวังดีมีสิทธิ์เข้าถึง virtual machine โดยที่ไม่ได้เป็นผู้ดูแลระบบ ทำการเปิดใช้งานกราฟิก 3D ซึ่งจะสามารถโจมตีในรูปแบบ denial of service ได้

– CVE-2024-22269 CVE-2024-22269 (CVSS score: 7.1) เป็นช่องโหว่การเปิดเผยข้อมูลในอุปกรณ์ Bluetooth ที่ทำให้ผู้ไม่หวังดีมีสิทธิ์เป็นผู้ดูแลระบบใน virtual machine จะสามารถอ่านข้อมูลในหน่วยความจำของ hypervisor จาก virtual machine ได้

– CVE-2024-22270 (CVSS score: 7.1) เป็นช่องโหว่การเปิดเผยข้อมูลในฟังก์ชัน Host Guest File Sharing (HGFS) ที่ทำให้ผู้ไม่หวังดีมีสิทธิ์เป็นผู้ดูแลระบบใน virtual machine จะสามารถอ่านข้อมูลในหน่วยความจำของ hypervisor จาก virtual machine ได้

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำผู้ใช้งานและผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบควรอัปเดตเป็นเวอร์ชันล่าสุดทันที และผู้ที่ไม่สามารถอัปเดตผลิตภัณฑ์ที่ได้รับผลกระทบทันทีควรปิดการสนับสนุน Bluetooth บน virtual machine และปิดใช้งานคุณลักษณะการเร่งความเร็ว 3D เพื่อป้องกันการถูกโจมตี หรือตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ หรือตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้นและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ 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-2024-050
2. https://thehackernews.com/2024/05/Vmware-patches-severe-security-flaws-in.html

TLP:CLEAR