

- Financial Damage
- Reputation Damage
- Non-compliance
- Privacy Violation

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability



## แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ VMware Workstation และ VMware Fusion (CVE-2024-22267, CVE-2024-22268, CVE-2024-22269 และ CVE-2024-22270)

วันที่แจ้งเตือน 24 พฤษภาคม 2567

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรง (Critical) ในผลิตภัณฑ์ VMware Workstation Pro / Player (Workstation) และ VMware Fusion รวมจำนวน 4 รายการ โดยมีรายละเอียดดังตาราง

CVE	Description	Affected	Fixed version
CVE-2024-22267	ช่องโหว่ use-after-free ในอุปกรณ์ vbluetooth ส่งผลให้ผู้ไม่หวังดีที่ถือสิทธิ์ระดับผู้ดูแลระบบ บน Virtual Machine จะสามารถใช้ช่องโหว่นี้ส่งคำสั่ง (execute code) เพื่อสร้าง process ใด ๆ ของ Virtual Machine บนเครื่อง Host ได้		
CVE-2024-22268	ช่องโหว่ heap buffer-overflow ในฟังก์ชัน Shader ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึง Virtual Machine ที่มีการเปิดใช้งานกราฟิก 3D เพื่อโจมตีในรูปแบบ denial of service ได้	VMware Workstation: (version 17.x)	VMware Workstation: Version 17.5.2
CVE-2024-22269	ช่องโหว่การเปิดเผยข้อมูลในอุปกรณ์ vbluetooth ส่งผลให้ผู้ไม่หวังดีที่ถือสิทธิ์ระดับผู้ดูแลระบบ บน Virtual Machine สามารถอ่านข้อมูลในหน่วยความจำ ของ hypervisor จาก Virtual Machine ได้	VMware Fusion: (version 13.x)	VMware Fusion: Version 13.5.2
CVE-2024-22270	ช่องโหว่การเปิดเผยข้อมูลในฟังก์ชัน Host Guest File Sharing (HGFS) ส่งผลให้ผู้ไม่หวังดีที่ถือสิทธิ์ระดับผู้ดูแลระบบบน Virtual Machine สามารถอ่านข้อมูลในหน่วยความจำ ของ hypervisor จาก Virtual Machine ได้		

ThaiCERT แนะนำผู้ใช้งาน และผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบควรอัปเดตเป็นเวอร์ชันล่าสุดทันที และผู้ที่ไม่สามารถอัปเดตผลิตภัณฑ์ที่ได้รับผลกระทบได้ ควรปิดการใช้งาน Bluetooth บน Virtual Machine และปิดใช้งาน Accelerate 3D graphics เพื่อป้องกันการถูกโจมตีหรือตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น

### ข้อมูลอ้างอิง

- 1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 23 พ.ค. 2567
- 2) <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24280>
- 3) <https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-050>
- 4) <https://thehackernews.com/2024/05/vmware-patches-severe-security-flaws-in.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ