วันที่ 9 กันยายน 2569

ช่องโหว่ร้ายแรงใน VMware Workstation และ Fusion เปิดทางให้ผู้ดูแล VM รันโค้ดบน Host ได้

Broadcom ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ 2 รายการที่ส่งผลกระทบต่อ VMware Workstation และ Fusion โดยหนึ่งในนั้นเป็นช่องโหว่ร้ายแรงที่อาจเปิดทางให้ผู้โจมตีสามารถรันโค้ดใดๆ ได้ภายใต้เงื่อนไขบางประการ ช่องโหว่นี้ถูกติดตามในชื่อ CVE-2026-59346 (คะแนน CVSS: 9.3) เป็นช่องโหว่ประเภท Integer Overflow ซึ่งผู้โจมตีที่มีสิทธิ์ระดับสูงบนเครื่องสามารถใช้เพื่อรันโค้ดใดๆ ได้ ผู้ไม่หวังดีที่มีสิทธิ์ระดับผู้ดูแลระบบภายในเครื่อง Virtual Machine ซึ่งใช้ Virtual Network Adapter แบบ VMXNET3 อาจใช้ช่องโหว่นี้เพื่อรันโค้ดบน Host ได้

บริษัทเทคโนโลยีรายใหญ่ให้เครดิตกับ @h4urek, @cameudis และ Stan S สำหรับการค้นพบช่องโหว่ดังกล่าว นอกจากนี้ Broadcom ยังได้แก้ไขช่องโหว่ Stack-Based Buffer Overflow ใน HGFS (CVE-2026-59347, คะแนน CVSS: 8.1) ซึ่งผู้ไม่หวังดีที่มีสิทธิ์ระดับผู้ดูแลระบบภายในเครื่อง Virtual Machine สามารถใช้ช่องโหว่นี้เพื่อรันโค้ดด้วยสิทธิ์ของ VMX Process ของ Virtual Machine ที่กำลังทำงานอยู่บน Host

ในทั้งสองกรณี การโจมตีให้สำเร็จจำเป็นต้องอาศัยการที่ผู้โจมตีมีสิทธิ์ระดับผู้ดูแลระบบภายในเครื่องอยู่ก่อนแล้ว อย่างไรก็ตาม สิทธิ์ดังกล่าวอาจถูกได้รับมาจากการโจมตีรูปแบบอื่น เช่น การหลอกลวงผ่าน Phishing หรือการใช้ประโยชน์จากการตั้งค่าของผู้ใช้ที่ไม่รัดกุม

ช่องโหว่ทั้งสองรายการส่งผลกระทบต่อ VMware Workstation และ VMware Fusion เวอร์ชัน 25H2 และ 26H1 โดย Broadcom ระบุว่าไม่มีวิธีแก้ไขชั่วคราว (Workaround) ที่สามารถป้องกันช่องโหว่ทั้งสองได้ พร้อมระบุว่าช่องโหว่ได้รับการแก้ไขแล้วใน VMware Workstation 26H1u1 และ VMware Fusion 26H1u1 แม้ในขณะนี้จะยังไม่มีหลักฐานว่าช่องโหว่ดังกล่าวถูกนำไปใช้โจมตีจริง แต่ช่องโหว่ในผลิตภัณฑ์ VMware ยังคงเป็นเป้าหมายที่กลุ่มผู้โจมตีให้ความสนใจเป็นอย่างมาก

เมื่อเดือนที่ผ่านมา มีการตรวจพบกลุ่มผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ 2 รายการใน VMware vCenter อย่างจริงจัง ได้แก่ CVE-2026-59309 และ CVE-2026-59310 โดยช่องโหว่รายการหลังถูกสงสัยว่าถูกนำไปพัฒนาเป็นเครื่องมือโจมตีโดยกลุ่ม Advanced Persistent Threat (APT) ที่เชื่อมโยงกับจีน

กิจกรรมการโจมตีดังกล่าวเริ่มต้นขึ้นเพียง 5 วันตามปฏิทินหลังจากมีการเปิดเผยช่องโหว่ต่อสาธารณะ และคาดว่าสามารถเจาะระบบ IP ของเหยื่อที่ไม่ซ้ำกันได้ 361 รายการใน 47 ประเทศ โดยการติดเชื้อส่วนใหญ่กระจุกตัวอยู่ในเยอรมนี (55 รายการ), สหรัฐฯ (41 รายการ), ตุรกี (38 รายการ), อิหร่าน (26 รายการ) และฝรั่งเศส (25 รายการ)

ข้อมูลอ้างอิง

Sep 5, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/09/critical-vmware-workstation-and-fusion.html