วันที่ 30 กรกฎาคม 2569

ช่องโหว่ร้ายแรง 3 รายการใน VMware เปิดทางให้ข้ามการยืนยันตัวตน รันโค้ด และหลบหนีออกจากเครื่องเสมือน (VM Escape)

Broadcom ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่ส่งผลกระทบต่อ VMware ESX, vCenter, Workstation และ Fusion โดยในจำนวนนี้มี 3 ช่องโหว่ที่ถูกจัดอยู่ในระดับ Critical

- ช่องโหว่ตัวแรกคือ CVE-2026-59309 (คะแนน CVSS: 9.8) ซึ่งเป็นช่องโหว่ Authentication Bypass ใน VMware vCenter Broadcom ระบุว่า ผู้ไม่หวังดีที่สามารถเข้าถึงเครือข่ายของ vCenter ได้ อาจใช้ช่องโหว่นี้เพื่อข้ามการยืนยันตัวตน และเข้าถึงระบบโดยไม่ได้รับอนุญาต
- ช่องโหว่ตัวที่สองคือ CVE-2026-59310 (คะแนน CVSS: 9.8) ซึ่งเป็นช่องโหว่ประเภท Directory Traversal ใน vCenter โดยผู้ไม่หวังดีที่สามารถเข้าถึงเครือข่ายได้ อาจใช้ช่องโหว่นี้เพื่อรันโค้ดที่เป็นอันตรายบนระบบ (Arbitrary Code Execution)

ทั้งสองช่องโหว่ได้รับการแก้ไขแล้วในเวอร์ชันดังต่อไปนี้

- VMware Cloud Foundation และ VMware vSphere Foundation เวอร์ชัน 9.1.x.x (แก้ไขในเวอร์ชัน 9.1.0.0300)
- VMware Cloud Foundation และ VMware vSphere Foundation เวอร์ชัน 9.0.x.x (แก้ไขในเวอร์ชัน 9.0.2.0100)
- VMware vCenter เวอร์ชัน 8.0 (แก้ไขในเวอร์ชัน 8.0 U3k)
- VMware Cloud Foundation เวอร์ชัน 5.x (ออกแพตช์แบบ Async ไปยังเวอร์ชัน 8.0 U3k)

นอกจากนี้ Broadcom ยังได้แก้ไขช่องโหว่อีก 3 รายการ ได้แก่

- **CVE-2026-47876 (คะแนน CVSS: 9.3):** ช่องโหว่แบบ Out-of-Bounds Write ในอะแดปเตอร์เครือข่ายเสมือน VMXNET3 ของ VMware ESX โดยผู้ไม่หวังดีที่มีสิทธิ์ผู้ดูแลระบบ (Local Administrator) ภายในเครื่องเสมือน (VM) สามารถใช้ช่องโหว่นี้เพื่อรันโค้ดบนเครื่องโฮสต์ (Host) ได้โดยตรง (แก้ไขแล้วใน VMware Cloud Foundation และ VMware vSphere Foundation เวอร์ชัน ESXi-9.1.0.0200-25557999 และ ESXi-9.0.2.0100-25595025 รวมถึง VMware ESX เวอร์ชัน ESXi80U3k-25595708)
- **CVE-2026-41703 (คะแนน CVSS: 7.6):** ช่องโหว่แบบ Out-of-Bounds Read ใน VMware ESX ซึ่งผู้ไม่หวังดีที่มีสิทธิ์ในการสร้างหรือปรับใช้เครื่องเสมือน (VM Deployment Privileges) สามารถใช้ช่องโหว่นี้เพื่อเปิดเผยข้อมูลหรือทำให้เกิดภาวะปฏิเสธการให้บริการ (Denial-of-Service: DoS) ได้ ส่วนใน VMware Workstation และ Fusion ผลกระทบจะจำกัดอยู่ที่การเปิดเผยข้อมูลเท่านั้น (แก้ไขแล้วใน VMware Cloud Foundation และ VMware vSphere Foundation เวอร์ชัน ESXi-9.1.0.0-25370933 และ ESXi-9.0.2.0100-25595025, VMware ESX เวอร์ชัน ESXi80U3i-25205845, VMware Workstation 26H1, VMware Fusion 26H1 และ VMware Cloud Foundation 5.2.3)
- **CVE-2026-41709 (คะแนน CVSS: 2.7):** ช่องโหว่ด้าน Insufficient Logging ใน VMware ESX ซึ่งผู้ดูแลระบบที่ประสงค์ร้ายสามารถดำเนินการบางอย่างได้โดยไม่ถูกบันทึกไว้ใน Log ของระบบ (แก้ไขแล้วใน VMware Cloud Foundation และ VMware vSphere Foundation เวอร์ชัน ESXi-9.1.0.0-25370933 และ ESXi-9.0.2.0100-25595025 รวมถึง VMware ESX เวอร์ชัน ESXi80U3j-25429389)

Broadcom ระบุว่า ขณะนี้ยังไม่พบหลักฐานว่าช่องโหว่เหล่านี้ถูกนำไปใช้โจมตีจริงอย่างไรก็ตาม บริษัทระบุว่า ไม่มีวิธีลดความเสี่ยงสำหรับช่องโหว่เหล่านี้ และได้จัดให้อัปเดตครั้งนี้เป็น Emergency Change ที่ควรดำเนินการอัปเดตโดยเร็วที่สุด

นอกจากนี้ Broadcom ยังระบุว่า CVE-2026-47876 เป็นช่องโหว่ประเภท Virtual Machine Escape (VM Escape) ซึ่งหมายความว่า ผู้โจมตีที่มีสิทธิ์ผู้ดูแลระบบภายในเครื่องเสมือน และเครื่องเสมือนนั้นใช้อะแดปเตอร์เครือข่าย VMXNET3 อาจสามารถรันโค้ดบนเครื่อง ESX Host ได้โดยตรง

ข้อมูลอ้างอิง

Jul 29, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html