วันที่ 27 มกราคม 2569

CISA เพิ่มช่องโหว่ VMware vCenter ที่ถูกโจมตีจริง CVE-2024-37079 เข้า KEV Catalog

สำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้ทำการเพิ่มช่องโหว่ที่มีความร้ายแรงสูงซึ่งส่งผลกระทบต่อ Broadcom VMware vCenter Server เข้าสู่รายการ Known Exploited Vulnerabilities (KEV) เมื่อวันศุกร์ที่ผ่านมา หลังจากพบหลักฐานยืนยันว่ามีการนำช่องโหว่นี้ไปใช้โจมตีจริงแล้วในโลกความเป็นจริง แม้ว่าช่องโหว่ดังกล่าวจะมีการออกแพตช์แก้ไขไปตั้งแต่เดือนมิถุนายน 2024 ก็ตาม

รายละเอียดเชิงเทคนิคของช่องโหว่ CVE-2024-37079 (CVSS 9.8)

ช่องโหว่รหัส CVE-2024-37079 ได้รับคะแนนความรุนแรงสูงถึง 9.8 จาก 10.0 โดยถูกระบุว่าเป็นปัญหาประเภท Heap Overflow ที่เกิดขึ้นในการทำงานของโปรโตคอล DCE/RPC

กลไกการโจมตีนี้อาจเปิดทางให้ผู้ไม่หวังดีที่สามารถเข้าถึงเครือข่ายของ vCenter Server ส่งแพ็กเก็ตที่ถูกออกแบบมาเป็นพิเศษ (Specially Crafted Packets) เพื่อทำการรันคำสั่งจากระยะไกล (Remote Code Execution - RCE) และเข้าควบคุมระบบที่ได้รับผลกระทบได้ทันที

ประวัติการค้นพบและชุดช่องโหว่ที่เกี่ยวข้อง

ช่องโหว่นี้ได้รับการแก้ไขโดย Broadcom ในเดือนมิถุนายน 2024 พร้อมกับอีกหนึ่งช่องโหว่คือ CVE-2024-37080 ซึ่งเป็นปัญหา Heap Overflow ในโปรโตคอล DCE/RPC เช่นเดียวกัน และอาจนำไปสู่การรันคำสั่งจากระยะไกลได้ โดยผู้ที่ค้นพบและรายงานช่องโหว่เหล่านี้คือ Hao Zheng และ Zibo Li นักวิจัยจากบริษัทด้านความปลอดภัยไซเบอร์ QiAnXin LegendSec ของจีน

จากการนำเสนอข้อมูลในงานประชุม Black Hat Asia เมื่อเดือนเมษายน 2025 นักวิจัยระบุว่าช่องโหว่ทั้งสองนี้เป็นเพียงส่วนหนึ่งของชุดช่องโหว่ทั้งหมด 4 รายการ ซึ่งประกอบด้วย:

- ช่องโหว่ Heap Overflow จำนวน 3 รายการ
- ช่องโหว่ยกระดับสิทธิ์ (Privilege Escalation) จำนวน 1 รายการ

ซึ่งทั้งหมดถูกพบในบริการ DCE/RPC โดยช่องโหว่อีกสองรายการที่เหลือคือ CVE-2024-38812 และ CVE-2024-38813 ได้รับการแก้ไขโดย Broadcom ตามมาในเดือนกันยายน 2024

ความอันตราย: การยึดสิทธิ์ Root และควบคุม ESXi

ประเด็นที่น่าสนใจและอันตรายอย่างยิ่งคือ นักวิจัยพบว่าช่องโหว่ Heap Overflow หนึ่งรายการสามารถนำไปใช้ร่วมกับช่องโหว่ยกระดับสิทธิ์ (CVE-2024-38813) เพื่อเข้าถึงสิทธิ์ระดับสูงสุด (root) จากระยะไกลโดยไม่ได้รับอนุญาต และท้ายที่สุดอาจสามารถเข้าควบคุมระบบ ESXi ได้ทั้งหมด

สถานการณ์การโจมตีและการยืนยันจาก Broadcom

ในปัจจุบันยังไม่ทราบแน่ชัดว่าช่องโหว่ CVE-2024-37079 ถูกนำไปใช้โจมตีในรูปแบบใด ใครเป็นผู้อยู่เบื้องหลัง หรือมีขอบเขตความเสียหายกว้างขวางเพียงใด อย่างไรก็ตามทาง Broadcom ได้อัปเดตคำแนะนำด้านความปลอดภัยของตนเองเพื่อยืนยันอย่างเป็นทางการแล้วว่ามีการใช้ช่องโหว่นี้โจมตีจริง โดยระบุในประกาศล่าสุดว่า “Broadcom มีข้อมูลที่บ่งชี้ว่ามีการนำช่องโหว่ CVE-2024-37079 ไปใช้โจมตีจริงแล้ว”

มาตรการบังคับใช้และข้อแนะนำ

จากสถานการณ์การโจมตีที่กำลังเกิดขึ้น หน่วยงานในกลุ่ม Federal Civilian Executive Branch (FCEB) ของสหรัฐฯ จึงถูกกำหนดให้ต้องดำเนินการอัปเดตระบบ vCenter Server เป็นเวอร์ชันล่าสุดให้เสร็จสิ้นภายในวันที่ 13 กุมภาพันธ์ 2026 เพื่อให้ได้รับการป้องกันที่เหมาะสมที่สุด

ข้อมูลอ้างอิง

Jan 24, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/cisa-adds-actively-exploited-vmware.html