วันที่ 7 สิงหาคม 2568

## Trend Micro ยืนยันพบการโจมตีช่องโหว่ร้ายแรงใน Apex One


Trend Micro ได้ออกคำเตือนและแนวทางบรรเทาปัญหาเพื่อแก้ไขช่องโหว่ด้านความปลอดภัยร้ายแรงใน Apex One Management Console เวอร์ชันติดตั้งในองค์กร (on-premise) ซึ่งบริษัทระบุว่าช่องโหว่นี้ถูกใช้โจมตีจริงแล้วในโลกไซเบอร์

ช่องโหว่ทั้งสองรายการคือ CVE-2025-54948 และ CVE-2025-54987 ได้รับคะแนนความรุนแรงสูงถึง 9.4 จากระบบ CVSS โดยถูกระบุว่าเป็นช่องโหว่ command injection ผ่าน management console และช่องโหว่การรันโค้ดจากระยะไกล (remote code execution)

“ช่องโหว่ใน management console ของ Trend Micro Apex One (แบบติดตั้งในองค์กร) อาจเปิดทางให้ผู้โจมตีจากระยะไกลที่ยังไม่ผ่านการยืนยันตัวตน สามารถอัปโหลดโค้ดอันตรายและสั่งรันคำสั่งบนระบบที่ได้รับผลกระทบได้” บริษัทไซเบอร์ซีเคียวริตี้กล่าวในประกาศเมื่อวันอังคาร

แม้ช่องโหว่ทั้งสองจะมีลักษณะคล้ายกัน แต่ CVE-2025-54987 นั้นมุ่งเป้าไปยังสถาปัตยกรรมซีพียูที่แตกต่างกัน โดยทีม Incident Response ของ Trend Micro และ Jacky Hsieh จาก CoreCloud Tech เป็นผู้รายงานช่องโหว่เหล่านี้

ขณะนี้ยังไม่มีข้อมูลเชิงลึกว่าแฮกเกอร์ใช้ช่องโหว่นี้ในการโจมตีอย่างไร แต่ Trend Micro ระบุว่า “พบอย่างน้อยหนึ่งกรณีที่มีความพยายามในการโจมตีช่องโหว่เหล่านี้จริง”

**แนวทางการแก้ไขและอัปเดต**

สำหรับเวอร์ชัน Apex One แบบให้บริการ (as a Service) ทางบริษัทได้ติดตั้งมาตรการป้องกันไว้เรียบร้อยแล้ว ตั้งแต่วันที่ 31 กรกฎาคม 2025 ส่วนเวอร์ชันติดตั้งภายในองค์กรนั้น ขณะนี้มีเครื่องมือแก้ไขชั่วคราวให้ใช้งาน และแพตช์อย่างเป็นทางการคาดว่าจะออกในช่วงกลางเดือนสิงหาคม 2025

อย่างไรก็ตาม Trend Micro ระบุว่า แม้เครื่องมือดังกล่าวจะสามารถป้องกันการโจมตีที่รู้จักได้ทั้งหมด แต่จะมีผลให้ผู้ดูแลระบบไม่สามารถใช้ฟังก์ชัน Remote Install Agent ในการติดตั้งเอเจนต์จาก Apex One Management Console ได้ โดยทางเลือกอื่น เช่น การติดตั้งผ่าน UNC path หรือไฟล์ติดตั้งเอเจนต์แบบแพ็กเกจยังคงใช้งานได้ตามปกติ

“โดยทั่วไปแล้ว การเจาะระบบผ่านช่องโหว่ลักษณะนี้ มักต้องอาศัยการเข้าถึงเครื่องที่มีช่องโหว่โดยตรง ไม่ว่าจะผ่านทางกายภาพหรือทางไกล” บริษัทกล่าวเพิ่มเติม “นอกเหนือจากการติดตั้งแพตช์และอัปเดตโซลูชันให้ทันสมัยแล้ว ลูกค้าควรตรวจสอบการเข้าถึงจากระยะไกลที่มีต่อระบบสำคัญ และมั่นใจว่านโยบายด้านความปลอดภัยและระบบป้องกันรอบขอบเครือข่ายได้รับการดูแลอย่างเหมาะสม”

**ข้อมูลอ้างอิง**

**Aug 6, 2025 By Ravie Lakshmanan**

- https://thehackernews.com/2025/08/trend-micro-confirms-active.html