วันที่ 13 มกราคม 2569

ช่องโหว่ RCE ใน Trend Micro Apex Central ได้คะแนน CVSS สูงถึง 9.8 ในเวอร์ชันติดตั้งบน Windows

Trend Micro ได้ดำเนินการออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่ส่งผลกระทบต่อ Apex Central สำหรับ Windows แบบติดตั้งภายในองค์กร (on-premise) โดยมีหนึ่งช่องโหว่ระดับร้ายแรงเป็นพิเศษ ซึ่งอาจเปิดทางให้ผู้โจมตีสามารถสั่งรันโค้ดใดก็ได้ (Remote Code Execution) บนระบบที่ได้รับผลกระทบ

เจาะลึกช่องโหว่ระดับวิกฤต CVE-2025-69258 (CVSS 9.8)

ช่องโหว่ดังกล่าวถูกติดตามด้วยรหัส CVE-2025-69258 และได้รับคะแนนความรุนแรงสูงถึง 9.8 จาก 10.0 โดยถูกอธิบายว่าเป็นปัญหาการรันโค้ดจากระยะไกลที่เกี่ยวข้องกับการทำงานของ LoadLibraryEX

ทาง Trend Micro ได้ระบุรายละเอียดว่า “ช่องโหว่ LoadLibraryEX ใน Trend Micro Apex Central อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ไม่ต้องยืนยันตัวตน สามารถโหลดไฟล์ DLL ที่ผู้โจมตีควบคุมเองเข้าไปในไฟล์โปรแกรมหลัก ส่งผลให้โค้ดของผู้โจมตีถูกรันภายใต้ สิทธิ์ระดับ SYSTEM บนระบบที่ได้รับผลกระทบ”

การแก้ไขช่องโหว่เพิ่มเติมอีก 2 รายการ

นอกจากนี้ Trend Micro ยังได้แก้ไขช่องโหว่อีก 2 รายการที่มีความรุนแรงระดับสูง ได้แก่:

- CVE-2025-69259 (CVSS: 7.5): ช่องโหว่จากการไม่ตรวจสอบค่า NULL ในข้อความบางประเภท ซึ่งอาจทำให้ผู้โจมตีจากระยะไกลที่ไม่ต้องยืนยันตัวตน สามารถทำให้ระบบไม่สามารถให้บริการได้ (Denial of Service - DoS)
- CVE-2025-69260 (CVSS: 7.5): ช่องโหว่การอ่านข้อมูลเกินขอบเขต (Out-of-bounds read) ซึ่งอาจถูกใช้เพื่อทำให้ระบบไม่สามารถให้บริการได้ (DoS) เช่นเดียวกัน

รายละเอียดเชิงเทคนิคในการโจมตี

บริษัท Tenable ซึ่งเป็นผู้ค้นพบและรายงานช่องโหว่ทั้งหมดนี้ตั้งแต่เดือนสิงหาคม 2025 ได้เปิดเผยว่า ผู้โจมตีสามารถใช้ประโยชน์จาก CVE-2025-69258 ได้โดยการส่งข้อความหมายเลข “0x0a8d” (“SC_INSTALL_HANDLER_REQUEST”) ไปยังโปรเซส MsgReceiver.exe ซึ่งจะส่งผลให้ระบบโหลดไฟล์ DLL ที่ผู้โจมตีควบคุมเข้าไป และรันโค้ดด้วยสิทธิ์ระดับสูงทันที

ในลักษณะเดียวกัน ช่องโหว่ CVE-2025-69259 และ CVE-2025-69260 สามารถถูกกระตุ้นได้โดยการส่งข้อความที่ถูกออกแบบมาเป็นพิเศษหมายเลข “0x1b5b” (“SC_CMD_CGI_LOG_REQUEST”) ไปยังโปรเซส MsgReceiver.exe ตัวเดิม ซึ่งรับฟังการเชื่อมต่ออยู่ที่ พอร์ต TCP เริ่มต้นหมายเลข 20001

เวอร์ชันที่ได้รับผลกระทบและเงื่อนไขการโจมตี

ช่องโหว่ทั้งหมดนี้ส่งผลกระทบต่อ Apex Central แบบ on-premise ที่มีเวอร์ชันต่ำกว่า Build 7190 ทั้งนี้ Trend Micro ระบุว่า การโจมตีจะประสบความสำเร็จได้ ผู้โจมตีจำเป็นต้องมีการเข้าถึงเครื่องเป้าหมายอยู่ก่อนแล้ว ไม่ว่าจะเป็นการเข้าถึงโดยตรงหรือการเข้าถึงจากระยะไกลก็ตาม

ข้อแนะนำและแนวทางการป้องกัน

Trend Micro แนะนำเพิ่มเติมว่า “นอกจากการติดตั้งแพตช์และอัปเดตโซลูชันอย่างทันท่วงทีแล้ว ลูกค้าควรตรวจสอบการเข้าถึงระบบสำคัญจากระยะไกล และตรวจให้แน่ใจว่านโยบายความปลอดภัยและระบบป้องกันเครือข่ายยังเป็นปัจจุบันอยู่เสมอ”

ข้อมูลอ้างอิง

Jan 9, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/trend-micro-apex-central-rce-flaw.html