แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Trend Micro ออก Security Patch แก้ไขช่องโหว่ในผลิตภัณฑ์ Apex One (CVE-2025-71210, CVE-2025-71211)

วันที่แจ้งเตือน 2 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Trend Micro ประกาศออก Security Patch เพื่อแก้ไขช่องโหว่ CVE-2025-71210 และ CVE-2025-71211 ในผลิตภัณฑ์ Trend Micro Apex One

ช่องโหว่ดังกล่าวเป็นประเภท Path Traversal ภายใน Apex One Management Console ส่งผลให้ผู้ไม่ประสงค์ดีสามารถสั่งรันโค้ดจากระยะไกล (Remote Code Execution: RCE) บนระบบ Windows ที่ยังไม่ได้ติดตั้งแพตช์ได้ และสามารถเข้าถึง Management Console ได้ โดยบริษัทผู้พัฒนาผลิตภัณฑ์ได้ออกแพตช์แก้ไขช่องโหว่ในเวอร์ชัน SaaS Apex One และออก Critical Patch Build 14136

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการอัปเดต Security Patch ตามที่ผู้ผลิตให้คำแนะนำ และตรวจสอบ Log และกิจกรรมที่ผิดปกติบนอุปกรณ์เครือข่าย รวมทั้ง ทบทวนการดำเนินการมาตรการ Cybersecurity ให้มีประสิทธิภาพอย่างสม่ำเสมอ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/trend-micro-warns-of-critical-apex-one-rce-vulnerabilities/
2. https://success.trendmicro.com/en-US/solution/KA-0022458