

แจ้งเตือนเพื่อเฝ้าระวังช่องโหว่

ในผลิตภัณฑ์ SolarWinds (CVE-2026-28326)

วันที่แจ้งเตือน 25 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบช่องโหว่ร้ายแรงในผลิตภัณฑ์ SolarWinds Access Rights Manager (ARM) (CVE-2026-28326) และอาจส่งผลให้ผู้ไม่หวังดีสามารถส่งรันท้าสั่งบนระบบที่ได้รับผลกระทบได้

ช่องโหว่	ผลกระทบ
CVE-2026-28326 เป็นช่องโหว่ใน SolarWinds ARM ซึ่งเป็นระบบที่ใช้บริหารจัดการและตรวจสอบสิทธิการเข้าถึงทรัพยากร โดยช่องโหว่เกิดจากการใช้ Hard-coded Static Key หรือค่ากุญแจที่ถูกกำหนดไว้ภายในซอฟต์แวร์ ซึ่งอาจเปิดโอกาสให้ผู้โจมตีใช้ประโยชน์จากค่าดังกล่าว เพื่อหลีกเลี่ยงกลไกด้านความปลอดภัยบางส่วน และนำไปสู่การดำเนินการบนระบบโดยไม่จำเป็นต้องผ่านการยืนยันตัวตนก่อน	ผลิตภัณฑ์ที่ได้รับผลกระทบ: - SolarWinds Access Rights Manager เวอร์ชัน 2026.2 และก่อนหน้า - ระบบที่ยังไม่ได้อัปเดตเป็นเวอร์ชัน 2026.2.1 - ระบบที่เชื่อมต่อกับบริการบริหารสิทธิ์ เช่น Active Directory, File Server, ระบบ Identity and Access Management (IAM) อื่น ๆ ผลกระทบที่อาจเกิดขึ้นหากโจมตีสำเร็จ - ส่งรันท้าสั่งจากระยะไกล (Remote Code Execution) - เข้าถึงหรือแก้ไขข้อมูลในระบบ ARM มีสิทธิจัดการ - เข้าถึงข้อมูลบัญชีผู้ใช้และสิทธิการใช้งานภายในองค์กร - ใช้ ARM เป็นจุดเริ่มต้นเพื่อขยายการโจมตีไปยังระบบอื่นในเครือข่าย - ส่งผลกระทบต่อ Confidentiality, Integrity และ Availability (CIA) ของข้อมูลและระบบงานสำคัญ
คำแนะนำ: - ตรวจสอบเวอร์ชัน SolarWinds ARM ที่ใช้งานอยู่ หากยังใช้เวอร์ชัน 2026.2 หรือเก่ากว่า ให้พิจารณาอัปเดตเป็น 2026.2.1 หรือใหม่กว่า - จำกัดการเข้าถึง ARM จากภายนอกองค์กร - ตรวจสอบ Log เพื่อหากิจกรรมผิดปกติ - ตรวจสอบการเปลี่ยนแปลงสิทธิผู้ใช้งานย้อนหลัง - ตรวจสอบ Active Directory และระบบที่เชื่อมต่อกับ ARM - สำรองข้อมูลและทดสอบกระบวนการกู้คืนระบบ	

ข้อมูลอ้างอิง

1. <https://thehackernews.com/2026/09/solarwinds-patches-arm-hard-coded-key.html?>

2. <https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28326>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

TCM-CERT
Thai Capital Market CERT

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ