แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือนช่องโหว่ร้ายแรงใน plugin ของโปรแกรม WordPress (CVE-2026-1357)

**วันที่แจ้งเตือน 19 กุมภาพันธ์ 2569**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงใน plugin ของโปรแกรม WordPress (CVE-2026-1357) ได้แก่ Wpvivid Backup & Migration plugin ซึ่งเป็น plugin ที่ใช้สำหรับการย้ายเว็บไซต์ (Site Migrations) และการถ่ายโอนข้อมูลสำรอง (Backup Transfers) ระหว่างเซิร์ฟเวอร์

ช่องโหว่ดังกล่าวเป็นช่องโหว่ประเภท Improper Input Validation ซึ่งส่งผลให้ผู้ไม่หวังดีสามารถอัปโหลดไฟล์อันตรายเข้าสู่ระบบและสั่งรันคำสั่งบนเซิร์ฟเวอร์จากระยะไกล (Remote Code Execution: RCE) ได้โดยไม่ต้องยืนยันตัวตน ส่งผลให้มีความเสี่ยงที่เว็บไซต์อาจถูกยึดและควบคุมได้

ทั้งนี้ เวอร์ชันของ plugin ที่ได้รับผลกระทบ ได้แก่

- WPvivid Backup & Migration ทุกเวอร์ชันก่อนหน้า 0.9.124

**แนวทางป้องกันและแก้ไข**

- ดำเนินการอัปเดต WPvivid Backup & Migration plugin เป็นเวอร์ชันล่าสุดทันที (เวอร์ชัน 0.9.124)
- ตรวจสอบ Log การทำงานของเว็บเซิร์ฟเวอร์ และไฟล์ที่ถูกอัปโหลดผิดปกติ
- ตรวจสอบบัญชีผู้ใช้งานในระบบ WordPress ว่ามีการสร้างบัญชีผู้ดูแลระบบโดยไม่ได้รับอนุญาตหรือไม่
- จำกัดสิทธิการอัปโหลดไฟล์ และปิดการทำงานของฟังก์ชันที่ไม่จำเป็น
- สำรองข้อมูลเว็บไซต์และจัดเก็บไว้ในแหล่งที่ปลอดภัย

**การเฝ้าระวังและตรวจสอบความผิดปกติ**

- ตรวจสอบการร้องขอ HTTP ที่ผิดปกติ โดยเฉพาะคำสั่งที่เกี่ยวข้องกับการอัปโหลดไฟล์สำรองข้อมูล
- เฝ้าระวังไฟล์นามสกุล .php หรือไฟล์สคริปต์ที่ถูกสร้างขึ้นใหม่ ในโฟลเดอร์ uploads
- ตรวจสอบพฤติกรรม Web Shell หรือการเชื่อมต่อออกไปยัง IP Address ปลายทางที่ไม่ทราบแหล่งที่มา

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

**ข้อมูลอ้างอิง**


1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 18 ก.พ. 2569
2) https://www.bleepingcomputer.com/news/security/wordpress-plugin-with-900k-installs-vulnerable-to-critical-rce-flaw/?
3) https://nvd.nist.gov/vuln/detail/CVE-2026-1357