แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ใหม่ในผลิตภัณฑ์ PHP (CVE-2026-115560) หลังการออกแพตช์ฉุกเฉินเพื่อรับมือกับ PHP2Shell

วันที่แจ้งเตือน 29 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์กรณีพบรายงานช่องโหว่ใหม่ CVE-2026-115560 ใน PHP ซึ่งผู้ไม่หวังดีสามารถสั่งรันคำสั่งบนเว็บเซิร์ฟเวอร์ได้จากระยะไกล (Remote Code Execution: RCE) โดยช่องโหว่นี้ยังไม่มีแพตช์แก้ไข

ช่องโหว่	ผลกระทบ
• CVE-2026-115560 เป็นช่องโหว่ที่เกี่ยวข้องกับการจัดการ Session ของ PHP และอาจนำไปสู่ Remote Code Execution (RCE) • ผู้ไม่หวังดีสามารถสั่งรันคำสั่งบนเว็บเซิร์ฟเวอร์โดยไม่ได้รับอนุญาต • ช่องโหว่เกิดขึ้นเมื่อระบบมีการตั้งค่า Session ในรูปแบบเฉพาะ* และยังเปิดใช้งาน Session Upload Progress อยู่ • **ยังไม่มีแพตช์แก้ไขในขณะนี้** โดย PHP ระบุว่าจะเผยแพร่รายละเอียดฉบับเต็มและการแก้ไขพร้อม Bugfix Release รอบถัดไป ***เงื่อนไขที่ทำให้ระบบมีความเสี่ยง:** • เว็บแอปพลิเคชันที่ใช้งาน PHP และมีการตั้งค่า session.serialize_handler เป็น php_binary หรือ php_serializ • เว็บแอปพลิเคชันที่มีการเปลี่ยนค่า session.serialize_handler เป็น php ผ่านฟังก์ชัน ini_set() ระหว่างการทำงาน ก่อนเรียกใช้ session start() • ระบบที่เปิดใช้งานฟังก์ชัน Session Upload Progress • ระบบที่เปิดให้บริการผ่านอินเทอร์เน็ต ควรเร่งตรวจสอบการตั้งค่าและประเมินความเสี่ยงจากการถูกโจมตี	**ผลกระทบที่อาจเกิดขึ้น:** • ผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่เพื่อรันโค้ดอันตรายบนเว็บเซิร์ฟเวอร์โดยไม่ได้รับอนุญาต (Remote Code Execution: RCE) หากระบบมีการตั้งค่าตรงตามเงื่อนไขของช่องโหว่ • ผู้ไม่หวังดีอาจเข้าถึง แก้ไข หรือเปลี่ยนแปลงข้อมูลและการทำงานของเว็บแอปพลิเคชัน ภายใต้สิทธิของ PHP • ผู้ไม่หวังดีอาจใช้ระบบที่ได้รับผลกระทบในการดำเนินกิจกรรมที่เป็นอันตรายเพิ่มเติม ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการของระบบ

แนวทางการป้องกันและรับมือ:

- ตรวจสอบการตั้งค่า Session ของเว็บแอปพลิเคชัน โดยเฉพาะการกำหนดค่า session.serialize_handler และการเปลี่ยนแปลงค่าดังกล่าวระหว่างการทำงาน เพื่อประเมินความเสี่ยงจากช่องโหว่
- ปิดใช้งานฟังก์ชัน Session Upload Progress ชั่วคราว โดยกำหนดค่า session.upload_progress.enabled=0 ในการตั้งค่า PHP ตามคำแนะนำของผู้พัฒนา จนกว่าจะมีการเผยแพร่เวอร์ชันแก้ไขช่องโหว่
- ตรวจสอบการทำงานของเว็บแอปพลิเคชันหลังปรับการตั้งค่า เพื่อตรวจสอบว่าระบบยังสามารถทำงานได้ตามปกติ โดยเฉพาะฟังก์ชันที่เกี่ยวข้องกับการแสดงความคืบหน้าการอัปโหลดไฟล์
- หลีกเลี่ยงการเปลี่ยนแปลงการตั้งค่า Session ระหว่างการทำงาน หากไม่มีความจำเป็น และตรวจสอบให้การจัดการ Session เป็นไปอย่างถูกต้อง
- เฝ้าระวังและตรวจสอบความผิดปกติของระบบ โดยเฉพาะบันทึกการทำงานของเว็บเซิร์ฟเวอร์และ PHP พร้อมติดตามประกาศด้านความปลอดภัยจากผู้พัฒนา เพื่อดำเนินการอัปเดตเมื่อมีการเผยแพร่เวอร์ชันแก้ไขอย่างเป็นทางการ

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 29 ต.ค. 2569
2. https://thehackernews.com/2026/10/urgent-php-warns-of-another-unpatched.html?

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ