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

แนวทางการลดความเสี่ยงจากช่องโหว่ PHP2Shell

วันที่แจ้งเตือน 6 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณี PHP ออกแพตช์ฉุกเฉินแก้ไขช่องโหว่ PHP2Shell ซึ่งเป็นช่องโหว่ระดับวิกฤตใน PHP Runtime ซึ่งเป็นซอฟต์แวร์พื้นฐานที่ถูกใช้งานอย่างแพร่หลายในการให้บริการเว็บไซต์และเว็บแอปพลิเคชัน (CVE-2026-109618, CVE-2026-109619) เมื่อวันที่ 22 ตุลาคม 2569 และปัจจุบันศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“ThaiCERT สกมช.”) ได้เผยแพร่เอกสารแนะนำการตรวจสอบระบบที่ใช้งาน PHP เพื่อลดความเสี่ยงจากช่องโหว่ PHP2Shell (ข้อมูลอ้างอิง 3) โดยพิจารณาดำเนินการ ดังนี้

1) สำรวจการใช้งาน PHP ให้ครอบคลุมทุกระบบ โดยตรวจสอบเว็บไซต์ เว็บแอปพลิเคชัน ระบบงานภายในองค์กร ระบบ API, Hosting Control Panel, อุปกรณ์ที่มีหน้าเว็บไซต์บริหารจัดการ, Container/Docker Image รวมถึงระบบ Development, UAT, Staging, DR และระบบที่อยู่ภายใต้การดูแลของผู้ให้บริการภายนอก เนื่องจากการอัปเดตระบบ Web Server หรือ Application อาจยังไม่ครอบคลุม PHP ที่เป็นส่วนประกอบของระบบอื่น ๆ

2) ตรวจสอบเวอร์ชันและเร่งติดตั้ง Security Update โดยตรวจสอบ PHP ที่ใช้งานและติดตั้งเวอร์ชันที่ได้รับการแก้ไขช่องโหว่ CVE-2026-109618 และ CVE-2026-109619 แล้ว ได้แก่ PHP 8.2.35, 8.3.36, 8.4.27 และ 8.5.12 หรือใหม่กว่าที่ได้รับการสนับสนุนจากผู้ผลิต ทั้งนี้ สำหรับ PHP 8.1 หรือเวอร์ชันที่ต่ำกว่า ควรตรวจสอบแพตช์จากผู้ผลิตระบบปฏิบัติการหรือผู้ให้บริการที่เกี่ยวข้อง

3) สำรองข้อมูลและทดสอบก่อนทำการอัปเดต โดยสำรองฐานข้อมูล แอปพลิเคชัน และไฟล์ตั้งค่าที่เกี่ยวข้อง พร้อมทั้งจัดเตรียมแผนกู้คืน และทดสอบความเข้ากันได้ของแอปพลิเคชันก่อนนำแพตช์ขึ้นระบบ Production

4) ตรวจสอบระบบหลังอัปเดต หลังติดตั้งแพตช์ ให้เริ่มบริการ PHP/PHP-FPM หรือ Web Server ที่เกี่ยวข้องใหม่ เพื่อให้มั่นใจว่าไม่มี Process ที่ยังใช้ PHP เวอร์ชันก่อนทำการอัปเดต และทดสอบการเข้าสู่ระบบ การเชื่อมต่อฐานข้อมูล และฟังก์ชันสำคัญของระบบ พร้อมบันทึกหลักฐานเวอร์ชันแพตช์ วันที่ดำเนินการ และผู้รับผิดชอบ

5) กรณียังไม่สามารถอัปเดตได้ ควรมีมาตรการชั่วคราวเพื่อลดความเสี่ยง เช่น จำกัดการเข้าถึงระบบเฉพาะเครือข่ายหรือผู้ใช้งานที่จำเป็น ปิดบริการที่ไม่ใช้งาน และเพิ่มมาตรการติดตามและตรวจสอบ Log หรือพฤติกรรมการเข้าถึงที่ผิดปกติ เป็นต้น โดยมาตรการเหล่านี้ควรใช้เป็นการชั่วคราว และไม่ควรใช้ทดแทนการติดตั้งแพทช์รักษาความมั่นคงปลอดภัย

ผู้ประกอบธุรกิจและผู้ดูแลระบบสามารถดาวน์โหลดเอกสารคำแนะนำและเครื่องมือสำหรับตรวจสอบระบบที่มีการใช้งาน PHP รวมถึงตรวจสอบช่องโหว่ที่เกี่ยวข้อง เพื่อใช้ประกอบการสำรวจและประเมินความเสี่ยงของระบบ โดยสามารถศึกษารายละเอียดวิธีการใช้งาน และคู่มือประกอบได้จาก ThaiCERT สกมช. URL: https://dg.th/cunhqjf0al

สำนักงาน ก.ล.ต. และ TCM-CERT ตระหนักถึงความเสี่ยงจากช่องโหว่ดังกล่าว ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการของหน่วยงานในภาคตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวเพื่อให้บริษัทพิจารณาตรวจสอบระบบที่เกี่ยวข้องและดำเนินการมาตรการป้องกันและลดความเสี่ยงตามความเหมาะสม เพื่อป้องกันหรือลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินธุรกิจ

ข้อมูลอ้างอิง

1. จดหมายแจ้งเตือนภัยคุกคามทางไซเบอร์ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ วันที่ 22 ตุลาคม 2569
2. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 3 พฤศจิกายน 2569
3. ข่าวสารภัยคุกคามทางไซเบอร์ ThaiCERT สกมช. วันที่ 28 ตุลาคม 2569 (https://www.thaicert.or.th/2026/10/28/thaicert-ขอแนะนำหน่วยงานเร่งตร/)