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

Microsoft เตือนภัยคุกคาม PHP Web shell รูปแบบใหม่ ผ่าน HTTP Cookie

วันที่แจ้งเตือน 6 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft ได้เปิดเผยเทคนิคการโจมตีรูปแบบใหม่ที่ผู้ไม่หวังดีใช้ HTTP cookie เป็นช่องทางควบคุมการทำงานของ PHP Web shell บนระบบปฏิบัติการ Linux ในการรันคำสั่งจากระยะไกล (Remote Code Execution: RCE) และการคงอยู่ในระบบ (persistence) โดยไม่ถูกตรวจจับ

รายงานระบุว่า Web shell ดังกล่าวถูกออกแบบให้ใช้ค่า cookie เป็นตัวกำหนดเงื่อนไขในการทำงาน โดยโค้ดอันตรายจะอยู่ในสถานะไม่ทำงาน และจะเริ่มทำงานเมื่อได้รับ HTTP request ที่มีค่า cookie ตรงตามเงื่อนไขที่ผู้ไม่หวังดีกำหนด ช่วยให้หลีกเลี่ยงการตรวจจับได้ เนื่องจากเป็นวิธีการสื่อสารของเว็บตามปกติและยากต่อการแยกแยะจากทราฟฟิกที่ถูกต้อง นอกจากนี้ ยังพบว่าผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ ทำการติดตั้ง Web shell และตั้งค่า cron job เพื่อเรียกใช้งาน loader อย่างต่อเนื่อง และหาก Web shell ถูกลบ ระบบจะซ่อมแซม Web shell ดังกล่าวขึ้นใหม่ได้ ส่งผลให้ผู้ไม่หวังดีสามารถคงการเข้าถึงระบบได้ในระยะยาว

เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้น สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบเฝ้าระวังและตรวจสอบพฤติกรรมที่ผิดปกติของระบบเว็บแอปพลิเคชัน โดยเฉพาะการใช้งาน cookie ที่มีลักษณะผิดปกติหรือมีการเข้ารหัสซับซ้อน รวมถึงตรวจสอบไฟล์ PHP และสคริปต์ที่ไม่รู้จักในระบบอย่างสม่ำเสมอ ควบคู่กับการตรวจสอบ cron job และ scheduled tasks ที่อาจถูกใช้เป็นช่องทางในการเรียกใช้งานโค้ดอันตราย นอกจากนี้ ควรติดตั้งระบบตรวจจับและป้องกันการบุกรุกและ Web Application Firewall (WAF) ที่สามารถตรวจจับพฤติกรรมผิดปกติและตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/microsoft-details-cookie-controlled-php.html
2. https://www.microsoft.com/en-us/security/blog/2026/04/02/cookie-controlled-php-webshells-tradecraft-linux-hosting-environments/