แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ใน CMS Joomla และส่วนขยาย

วันที่แจ้งเตือน 14 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีช่องโหว่โหว่ที่เกี่ยวข้องกับ Joomla ครอบคลุมทั้งช่องโหว่ใน Joomla Core/Framework และช่องโหว่ในส่วนขยายของ Joomla ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของเว็บไซต์โดยตรง มีรายละเอียดดังนี้

การโจมตี	ผลกระทบ
• ผู้ไม่หวังดีสแกนหาเว็บไซต์ Joomla ที่เปิดให้บริการผ่านอินเทอร์เน็ต และตรวจสอบเวอร์ชันของ Joomla Core รวมถึงส่วนขยายที่ติดตั้งอยู่ • กรณีช่องโหว่ประเภท file upload : ผู้ไม่หวังดีสามารถอัปโหลดไฟล์ PHP, web shell หรือ backdoor ไปยังโฟลเดอร์ของเว็บไซต์ เพื่อสั่งรันคำสั่งบนเครื่องแม่ข่ายและใช้สิทธิเข้าถึงระบบ • กรณีช่องโหว่ SQL Injection : ผู้ไม่หวังดีสามารถใช้คำขอที่ถูกสร้างขึ้นเพื่ออ่าน แก้ไข หรือดึงข้อมูลจากฐานข้อมูลของเว็บไซต์ • กรณีช่องโหว่ XSS : ผู้ไม่หวังดีสามารถแทรกสคริปต์อันตรายเพื่อขโมย session ของผู้ดูแลระบบ หลอกให้ผู้ใช้งานดำเนินการบางอย่าง หรือเปลี่ยนเส้นทางผู้เข้าชมไปยังเว็บไซต์อันตราย • กรณีช่องโหว่ด้านการควบคุมสิทธิ การยกระดับสิทธิ หรือการข้าม MFA : ผู้ไม่หวังดีอาจสร้างหรือแก้ไขบัญชีผู้ดูแลระบบ และเปลี่ยนแปลงค่าการทำงานของเว็บไซต์โดยไม่ได้รับอนุญาต **สแกนหาเป้าหมาย ⟶ ใช้ประโยชน์จากช่องโหว่ ⟶ เข้าระบบ ⟶ ยกระดับสิทธิ ⟶ ควบคุมเว็บไซต์ ⟶ ขโมยข้อมูล/แพร่มัลแวร์ ⟶ ขยายการโจมตี**	• ผู้ไม่หวังดีสามารถแก้ไขหน้าเว็บไซต์ เปลี่ยนแปลงเนื้อหา ติดตั้งมัลแวร์ ฝังสคริปต์ สร้างบัญชีผู้ดูแลระบบที่มีสิทธิระดับสูง ใช้เว็บไซต์เป็นฐานส่งสแปม, phishing, ทำ SEO spam หรือขยายผลไปยังเว็บไซต์อื่นบนเครื่องแม่ข่ายเดียวกัน หรือ เว็บไซต์ที่อยู่บน shared hosting เดียวกัน • ข้อมูลสำคัญของเว็บไซต์อาจถูกเข้าถึงหรือรั่วไหล เช่น ข้อมูลผู้ใช้งาน ข้อมูลจากแบบฟอร์ม ฐานข้อมูลเว็บไซต์ และข้อมูลเชื่อมต่อในไฟล์ configuration.php เป็นต้น • เวอร์ชั่นที่ได้รับผลกระทบดูได้จาก **เอกสารแนบ** **เว็บไซต์ล่ม บริการสะดุด และภาพลักษณ์หน่วยงานเสียหาย ⟶ หน่วยงานเสียความน่าเชื่อถือ**

แนวทางการป้องกันและลดความเสี่ยง

- สำรวจเว็บไซต์ Joomla ทั้งหมด และตรวจสอบเวอร์ชันที่ใช้งาน
- อัปเดต Joomla และส่วนขยาย เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้ว
- ลบหรือปิดใช้งานส่วนเสริมที่ไม่จำเป็น หรือไม่น่าเชื่อถือ
- เพิ่มความปลอดภัยบัญชีผู้ดูแลระบบ ด้วย MFA และรหัสผ่านที่รัดกุม
- จำกัดการเข้าถึงหน้า Administrator เฉพาะผู้ได้รับอนุญาต
- ตรวจสอบบัญชี Administrator และเปลี่ยนรหัสผ่านบัญชีผู้ดูแลระบบ รวมถึงรหัสผ่านฐานข้อมูล FTP/SFTP SSH Hosting Panel และ API key ที่เกี่ยวข้อง หากมีความเสี่ยงว่าระบบอาจถูกเข้าถึง
- ป้องกันการอัปโหลดและรันไฟล์อันตราย ในโฟลเดอร์อัปโหลด
- ตรวจหาไฟล์หรือโค้ดผิดปกติที่อาจเป็น Web Shell หรือ Backdoor หรือ ไฟล์ที่มีการ obfuscate ในโฟลเดอร์ของเว็บไซต์, ตรวจสอบไฟล์ .htaccess, index.php, configuration.php, template และ plugin ว่ามีโค้ดที่ถูกแก้ไขผิดปกติหรือไม่
- ตรวจสอบ Log อย่างสม่ำเสมอ เพื่อหาพฤติกรรมน่าสงสัย
- ใช้ WAF/ModSecurity rule และระบบเฝ้าระวังความปลอดภัย เพื่อลดความเสี่ยง
- สำรองข้อมูลและทดสอบการกู้คืน เป็นประจำ
- หากพบการบุกรุกให้แยกระบบ และดำเนินการตามแผน Incident Response ทันที

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 14 ก.ค. 2569
2. https://developer.joomla.org/security-centre.html?