แจ้งเตือน : ช่องโหว่

Critical

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

แจ้งเตือนพบการใช้ประโยชน์จากช่องโหว่ SQL Injection ใน Plugin WP-Automatic

วันที่แจ้งเตือน 3 พฤษภาคม 2567

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานแจ้งเตือน กรณีพบการใช้ประโยชน์จากช่องโหว่ SQL Injection ใน Plugin WordPress-Automatic ที่ CVE-2024-27956 คะแนน CVSS 9.9 ระดับ (critical) ซึ่งผู้โจมตีอาจใช้ประโยชน์จากช่องโหว่ดังกล่าว เข้าถึงเว็บไซต์โดยไม่ได้รับอนุญาตเพื่อสร้างบัญชีผู้ใช้งานระดับผู้ดูแลระบบ ทำการอัปโหลดไฟล์ที่เป็นอันตราย และเข้าควบคุมเว็บไซต์

ทั้งนี้ ผู้ประกอบธุรกิจที่ใช้งานผลิตภัณฑ์ WordPress ดังกล่าวสามารถแก้ไขปัญหาเบื้องต้น โดยการอัปเดต WP-Automatic เป็นเวอร์ชันล่าสุด ตรวจสอบบัญชีผู้ใช้งาน ลบบัญชีผู้ใช้งานที่ไม่ได้รับอนุญาตหรือน่าสงสัย และสำรองข้อมูลอย่างสม่ำเสมอเพื่อการกู้คืน พร้อมทั้งควรเฝ้าระวังตรวจสอบการทำงานของผลิตภัณฑ์ที่ใช้งาน รวมถึงกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 27 เม.ย. 2567
2) https://nvd.nist.gov/vuln/detail/CVE-2024-27956
3) https://wpscan.com/blog/new-malware-campaign-targets-wp-automatic-plugin/
4) https://www.csa.gov.sg/alerts-advisories/security-bulletins/2024/sb-2024-013