ประจำวันอังคารที่ 19 กรกฎาคม 2565

ช่องโหว่ของปลั๊กอิน wpbakery ใน wordpress ที่ยังไม่ได้ทำการแพทช์ ตกเป็นเป้าหมายของการโจมตีมากขึ้น

โดยทีมรักษาความปลอดภัย Wordfence ของ WordPress ได้ออกมาเตือนถึงการโจมตีที่มากขึ้นโดยพุ่งเป้าไปยังช่องโหว่ที่ไม่ได้รับการแพทช์ในส่วนเสริม Kaswara สำหรับปลั๊กอิน WordPress WPBakery Page Builder หมายเลข CVE-2021-24284 (คะแนน CVSS 10) ที่ได้เปิดเผยไปเมื่อเดือนเมษายน 2564 ซึ่งเป็นช่องโหว่ด้านความปลอดภัยระดับวิกฤตที่สำคัญ ทำให้ผู้โจมตีที่ไม่ผ่านการตรวจสอบสิทธิ์สามารถอัปโหลดไฟล์ PHP ที่เป็นอันตรายไปยังเว็บไซต์ที่มีช่องโหว่ เละสามารถเรียกใช้โค้ดจากระยะไกลได้ ซึ่งผู้โจมตีสามารถใช้ประโยชน์จากข้อบกพร่องเพื่อแทรกโค้ด JavaScript ที่เป็นอันตรายลงในไฟล์เพื่อใช้ในการติดตั้ง WordPress และเข้ายึดเว็บไซต์ที่มีช่องโหว่ได้อย่างสมบูรณ์ ซึ่งเมื่อค้นพบช่องโหว่นี้แล้ว Wordfence ได้ออกแจ้งเตือนผู้ดูแลเว็บไซต์ WordPress ว่าปลั๊กอินยังไม่มีโปรแกรมแก้ไขและขอให้ลบออกทันที

แม้ว่าจะผ่านไปแล้วกว่าหนึ่งปีนับตั้งแต่มีการเปิดเผยช่องโหว่ซีโร่เดย์ดังกล่าว แต่ยังพบว่ามีเว็บไซต์ระหว่าง 4,000 เว็บไซต์ถึง 8,000 เว็บไซต์ ยังคงใช้ปลั๊กอินนี้ต่อไป ซึ่งจะทำให้เว็บไซต์เหล่านั้น ตกเป็นเป้าหมายของการโจมตีจากผู้ไม่หวังดี โดยในช่วง 2 สัปดาห์ที่ผ่านมา Wordfence พบว่ามีการโจมตีที่พุ่งเป้าไปที่ช่องโหว่ดังกล่าว โดยเฉลี่ยประมาณ 440,000 ครั้งต่อวัน การโจมตีมาจากที่อยู่ IP ที่โจมตี 10,215 แห่ง โดยมีที่อยู่ IP 5แห่งที่รับผิดชอบการโจมตีส่วนใหญ่ โดย Wordfence อธิบายว่าผู้โจมตีกำลังตรวจสอบเว็บไซต์ WordPress มากกว่า 1.5 ล้านเว็บไซต์ เพื่อหาปลั๊กอินที่มีช่องโหว่ แต่ส่วนใหญ่ไม่ได้รับผลกระทบเนื่องจากไม่ได้ใช้ปลั๊กอินที่มีช่องโหว่ดังกล่าว ทั้งนี้ ปลั๊กอินได้ถูกปิดการใช้งาน และผู้พัฒนาไม่มีท่าทีที่จะพัฒนาแพทช์เพื่ออุดช่องโหว่ ดังนั้น ตัวเลือกที่ดีที่สุดคือการลบปลั๊กอิน Kaswara Modern WPBakery Page Builder Addons ออกไปจากเว็บไซต์ WordPress อย่างสมบูรณ์

ที่มาของข่าว : https://www.securityweek.com/unpatched-wpbakery-wordpress-plugin-vulnerability-increasingly-targeted-attacks