วันที่ 27 สิงหาคม 2569

Attackers Target miniOrange SAML Flaws That Can Grant WordPress Admin Access

ผู้โจมตีกำลังพยายามใช้ประโยชน์จากช่องโหว่ร้ายแรง 2 รายการในปลั๊กอิน Xecurify miniOrange SAML 2.0 Single Sign On ซึ่งเป็นช่องโหว่ที่สามารถโจมตีได้โดยไม่ต้องยืนยันตัวตน และเปิดทางให้ผู้โจมตีเข้าสู่ระบบในฐานะผู้ใช้ WordPress รายใดก็ได้ รวมถึงบัญชีผู้ดูแลระบบ

ช่องโหว่ดังกล่าว ซึ่งเปิดเผยโดย Patchstack มีรายละเอียดดังต่อไปนี้

- CVE-2026-61979 (คะแนน CVSS: 8.1) - ช่องโหว่ยกระดับสิทธิ์ที่สามารถโจมตีได้โดยไม่ต้องยืนยันตัวตน เกิดจากความผิดพลาดในการตรวจสอบอัลกอริทึมลายเซ็น (แก้ไขแล้วในเวอร์ชัน 17.0.5 สำหรับ Standard edition)
- CVE-2026-15981 (คะแนน CVSS: 9.8) - ช่องโหว่ Authentication Bypass ที่เกิดจากการยอมรับลายเซ็นที่มีรูปแบบไม่ถูกต้องว่าเป็นลายเซ็นที่ถูกต้อง (แก้ไขแล้วในเวอร์ชัน 17.0.6 สำหรับ Standard edition)

สาเหตุเกิดจากฟังก์ชัน mo_saml_validate_signature() ใช้การตรวจสอบค่า Boolean แบบหลวมกับค่าจำนวนเต็ม 3 สถานะที่ส่งกลับโดย openssl_verify() ของ PHP ทำให้ค่าที่ส่งกลับเป็น -1 ซึ่งหมายถึงการเกิดข้อผิดพลาด ถูกประเมินว่าเป็นค่าที่เป็นจริง และจึงถูกมองว่าเป็นการตรวจสอบลายเซ็นที่สำเร็จ ตามคำอธิบายของ CVE-2026-15981 บน CVE.org

ช่องโหว่นี้ทำให้ผู้โจมตีที่ไม่จำเป็นต้องยืนยันตัวตนสามารถเข้าสู่ระบบในฐานะผู้ใช้ WordPress ที่มีอยู่แล้วได้ รวมถึงผู้ดูแลระบบ โดยการส่ง SAMLResponse ที่สร้างขึ้นเป็นพิเศษ ซึ่งภายในมี NameID ที่ผู้โจมตีสามารถควบคุมได้ และค่าลายเซ็นที่ถูกทำให้ผิดรูปแบบโดยเจตนา เพื่อกระตุ้นให้เกิดข้อผิดพลาดในการประมวลผลของ OpenSSL และทำให้กระบวนการตรวจสอบถูกข้ามไปโดยสิ้นเชิง ส่งผลให้มีการเรียกใช้ wp_set_auth_cookie() สำหรับบัญชีเป้าหมาย

บริษัทด้านความปลอดภัยของ WordPress ระบุว่า DigitalOcean security team เป็นผู้รายงานช่องโหว่ดังกล่าว โดยผู้โจมตีสามารถสร้าง SAML response ที่มีลายเซ็นผิดรูปแบบและส่งไปยังปลั๊กอิน ทำให้ปลั๊กอินเข้าใจว่าลายเซ็นดังกล่าวถูกต้อง

มีรายงานว่าผู้ให้บริการโครงสร้างพื้นฐานบนคลาวด์รายนี้ค้นพบช่องโหว่หลังจากตรวจพบความพยายามเข้าสู่ระบบด้วยบัญชีผู้ดูแลระบบ WordPress ที่ผิดปกติจากภายนอกเครือข่ายที่ได้รับอนุญาต ผู้โจมตีได้ใช้ช่องโหว่เพื่อขโมย Admin session cookie ของ WordPress ไปแล้ว แต่ไม่สามารถดำเนินการต่อได้ เนื่องจากการทำงานภายในหน้า Admin ถูกจำกัดให้เข้าถึงได้จากเครือข่ายที่ได้รับอนุญาตเท่านั้น Patchstack ระบุ

มีการตรวจพบการสแกนจากที่อยู่ IP ต่อไปนี้

- 207.211.214.41
- 79.127.224.14
- 102.91.71.83
- 162.243.116.148
- 84.201.6.54
- 64.225.25.188

การแพร่กระจายของกิจกรรมดังกล่าวบ่งชี้ว่าเป็นการสแกนแบบวงกว้าง มากกว่าจะเป็นแคมเปญที่เจาะจงเป้าหมาย Patchstack กล่าวเพิ่มเติม ผู้ที่อยู่เบื้องหลังดูเหมือนจะส่ง Exploit ไปยังทุกเว็บไซต์ที่ติดตั้งปลั๊กอินนี้ โดยไม่ได้ตรวจสอบว่าปลั๊กอินเป็น edition หรือเวอร์ชันใด

ผู้ดูแลเว็บไซต์ WordPress ควรติดตั้งการอัปเดตความปลอดภัยล่าสุดเพื่อป้องกันระบบ โดยเฉพาะอย่างยิ่งเนื่องจากขณะนี้มีโค้ด Proof-of-Concept (PoC) ที่เปิดให้ใช้งาน ซึ่งช่วยให้ผู้โจมตีสามารถนำช่องโหว่เหล่านี้มาใช้ร่วมกันเพื่อยกระดับสิทธิ์เป็นผู้ดูแลระบบ และเข้าควบคุมเว็บไซต์ที่มีช่องโหว่ได้

ข้อมูลอ้างอิง

Aug 25, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/attackers-target-miniorange-saml-flaws.html