

วันที่ 27 ตุลาคม 2569

PHP ได้ออกแพ็กเกจติดตั้งสำหรับ Windows ชุดใหม่ เพื่อแก้ไขช่องโหว่ CVE-2026-111497



PHP ได้ออกแพ็กเกจติดตั้งสำหรับ Windows ชุดใหม่ ครอบคลุม PHP เวอร์ชัน 8.2 ถึง 8.5 เพื่อแก้ไขช่องโหว่ CVE-2026-111497 ในไลบรารีบีบอัดข้อมูล Brotli ที่มาพร้อมกับแพ็กเกจดังกล่าว โดยช่องโหว่นี้อาจทำให้ผู้โจมตีสร้างความเสียหายต่อข้อมูลในหน่วยความจำ และอาจนำไปสู่การรั่วไหลของข้อมูลที่เป็นอันตรายบนระบบได้

PHP ระบุว่า ช่องโหว่นี้สามารถถูกโจมตีผ่านส่วนขยาย cURL ได้ เมื่อมีการเปิดใช้งานฟังก์ชันคลายการบีบอัดข้อมูลจากการตอบกลับ HTTP โดยอัตโนมัติ แม้ว่า cURL จะปิดฟังก์ชันนี้ไว้เป็นค่าเริ่มต้น แต่แอปพลิเคชันและไลบรารีที่ใช้รับส่งข้อมูลผ่าน HTTP สามารถเปิดใช้งานได้

แพ็กเกจชุดใหม่ประกอบด้วยเวอร์ชัน 8.5.12-1, 8.4.27-1, 8.3.36-1 และ 8.2.35-1 ซึ่งถูกปล่อยออกมาเพียง 5 วันหลังจากการอัปเดตเมื่อวันที่ 21 ตุลาคม ที่ผ่านมา เพื่อแก้ไขช่องโหว่ PHP2Shell จำนวน 2 รายการ ซึ่งเปิดทางให้ผู้โจมตีรั่วไหลข้อมูลจากระยะไกลได้ โดยแพ็กเกจชุดใหม่นี้ยังคงใช้ซอร์สโค้ด PHP เดิม ทำให้การแก้ไขช่องโหว่ก่อนหน้านี้ยังคงมีผลอยู่ พร้อมอัปเดตไลบรารี Brotli เป็นเวอร์ชัน 1.2.1 ที่ได้รับการแก้ไขช่องโหว่แล้ว

PHP มีการเผยแพร่รายการส่วนประกอบของซอฟต์แวร์ หรือ Software Bill of Materials (SBOM) ควบคู่ไปกับแพ็กเกจแต่ละชุด เพื่อแสดงว่าภายในประกอบด้วยซอฟต์แวร์หรือไลบรารีใดบ้าง โดยรายการของแพ็กเกจ x64 Non Thread Safe ทั้ง 4 เวอร์ชันที่เผยแพร่เมื่อสัปดาห์ก่อน ระบุว่ามีการใช้ Brotli เวอร์ชัน 1.2.0 ซึ่งเป็นหนึ่งในเวอร์ชันที่ได้รับผลกระทบจากช่องโหว่นี้

PHP แนะนำให้ผู้ใช้งานบน Windows ดาวน์โหลดและติดตั้งแพ็กเกจชุดใหม่จากหน้าดาวน์โหลดอย่างเป็นทางการ อย่างไรก็ตาม เนื่องจากหมายเลขเวอร์ชันหลักของ PHP ไม่ได้เปลี่ยนแปลง การตรวจสอบด้วยคำสั่ง `php -v` จึงยังคงแสดงหมายเลขเวอร์ชันเดิมทั้งก่อนและหลังการอัปเดต โดยผู้ใช้งานสามารถสังเกตแพ็กเกจชุดใหม่ได้จากเลข -1 ที่เพิ่มเข้ามาในชื่อไฟล์ เช่น `php-8.5.12-1-nts-Win32-vs17-x64.zip` รวมถึงตรวจสอบค่า SHA-256 Hash ที่ระบุไว้บนหน้าดาวน์โหลด เพื่อยืนยันว่าเป็นแพ็กเกจชุดใหม่ที่ได้รับการแก้ไขแล้ว

การคลายการบีบอัดข้อมูลโดยอัตโนมัติ คือกระบวนการที่ cURL ส่งคำขอไปยังเซิร์ฟเวอร์เพื่อรับข้อมูลในรูปแบบที่ถูกบีบอัด ก่อนจะคลายการบีบอัดข้อมูลดังกล่าวโดยอัตโนมัติ โดยในโค้ด PHP สามารถเปิดใช้งานฟังก์ชันนี้ผ่านตัวเลือก `CURLOPT_ENCODING` และหากกำหนดค่าเป็นค่าว่าง ระบบจะยอมรับรูปแบบการบีบอัดทั้งหมดที่ cURL รองรับ

สำหรับ Guzzle ซึ่งเป็นไลบรารีที่ใช้รับส่งข้อมูลผ่าน HTTP ใน PHP พบว่ามีการกำหนดค่า `CURLOPT_ENCODING` เป็นค่าว่างโดยอัตโนมัติสำหรับคำขอที่ส่งผ่าน cURL ตามที่ปรากฏในซอร์สโค้ดของ Guzzle เวอร์ชัน 7.16.1 และ 8.3.1 จากข้อมูลดังกล่าวประกอบกับคำอธิบายของ PHP ทำให้มีความเป็นไปได้ว่าแอปพลิเคชันที่ใช้งาน Guzzle ด้วยการตั้งค่าเริ่มต้น จะเข้าข่ายเงื่อนไขที่สามารถถูกโจมตีผ่านช่องโหว่นี้ได้ หากยังใช้แพ็คเกจ PHP สำหรับ Windows ที่เผยแพร่เมื่อสัปดาห์ก่อน อย่างไรก็ตาม The Hacker News ระบุว่ายังไม่ได้ทดสอบสถานการณ์ดังกล่าวบนระบบ Windows จริง

การโจมตีสามารถเกิดขึ้นได้เมื่อแอปพลิเคชัน PHP ติดต่อไปยังเซิร์ฟเวอร์ และได้รับข้อมูลตอบกลับที่ถูกบีบอัดและสร้างขึ้นเป็นพิเศษเพื่อใช้โจมตีช่องโหว่นี้

Google ประเมินความรุนแรงของช่องโหว่นี้ไว้ที่ 9.2 จาก 10 คะแนน หรือระดับวิกฤต (Critical) ตามมาตรฐาน CVSS 4.0 ขณะที่ Red Hat ประเมินไว้ที่ 8.1 คะแนน หรือระดับสำคัญ (Important) ตามมาตรฐาน CVSS 3.1

นักวิจัยจาก Imperva สามารถใช้ประโยชน์จากช่องโหว่นี้เพื่อรันโค้ดบน Node.js เวอร์ชันทางการชุดหนึ่งได้สำเร็จ แม้ว่า จะต้องทดลองโจมตีหลายครั้งก็ตาม อย่างไรก็ตาม ประกาศของ PHP ไม่ได้ระบุว่าพบการนำช่องโหว่นี้ไปใช้โจมตีจริง ขณะที่ การประเมินของ CISA เมื่อวันที่ 23 ตุลาคม ระบุว่ายังไม่พบการใช้ประโยชน์จากช่องโหว่นี้ในการโจมตี และช่องโหว่ดังกล่าวยังไม่ถูกเพิ่มเข้าไปในรายการช่องโหว่ที่ถูกใช้โจมตีจริง หรือ Known Exploited Vulnerabilities (KEV) ณ วันที่มีการอัปเดตข้อมูล

ช่องโหว่นี้ถูกค้นพบโดยนักวิจัยจาก OpenAI ก่อนที่ Google จะออกอัปเดตแก้ไขใน Brotli เวอร์ชัน 1.2.1, 1.1.1 และ 1.0.10 เมื่อมีการเปิดเผยช่องโหว่ครั้งแรกในวันที่ 21 ตุลาคม นอกจากนี้ Node.js, Bun และซอฟต์แวร์อื่น ๆ ที่มีการรวมไลบรารี Brotli ไว้ภายใน ก็ได้ทยอยออกอัปเดตเพื่อแก้ไขช่องโหว่นี้แล้วเช่นกัน

ประกาศของ PHP ไม่ได้ระบุวิธีแก้ไขปัญหาล่วงหน้าสำหรับระบบที่ยังไม่สามารถติดตั้งอัปเดตได้ อย่างไรก็ตาม OpenAI แนะนำให้ปิดการคลายการบีบอัดข้อมูล Brotli โดยอัตโนมัติในโปรแกรมที่ใช้รับส่งข้อมูลผ่าน HTTP จนกว่าจะติดตั้งอัปเดตเรียบร้อยแล้ว พร้อมเตือนว่าการลบค่า `br` ซึ่งเป็นชื่อที่ใช้ระบุรูปแบบการบีบอัด Brotli ออกจากส่วนหัว Accept-Encoding เพียงอย่างเดียว ไม่สามารถป้องกันเซิร์ฟเวอร์จากการส่งข้อมูลในรูปแบบ Brotli กลับมาได้

สำหรับการใช้งานในโค้ด PHP สามารถทำตามคำแนะนำดังกล่าวได้ด้วยการไม่กำหนดค่า `CURLOPT_ENCODING` เนื่องจาก cURL จะไม่คลายการบีบอัดข้อมูลโดยอัตโนมัติหากไม่ได้เปิดใช้งานตัวเลือกนี้ ส่วนผู้ที่ใช้งาน Guzzle สามารถกำหนดตัวเลือก `decode_content` เป็น `false` เพื่อปิดการคลายการบีบอัดข้อมูลโดยอัตโนมัติทั้งหมด อย่างไรก็ตาม การตั้งค่านี้จะส่งผลต่อการบีบอัดรูปแบบอื่นด้วย เช่น gzip ซึ่งจะ使得แอปพลิเคชันได้รับข้อมูลที่ยังอยู่ในรูปแบบบีบอัดเช่นกัน

ข้อมูลอ้างอิง

Oct 26, 2026, By Swati Khandelwal

- <https://thehackernews.com/2026/10/php-issues-second-windows-security.html>