แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

WordPress และ VMware Avi Load Balancer ออก Security Patch เพื่อแก้ไขช่องโหว่หลายรายการ

วันที่แจ้งเตือน 23 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ และเผยแพร่ข่าวสาร กรณีช่องโหว่ใน WordPress Core จำนวน 2 รายการ ที่มีผู้ไม่หวังดีนำมาใช้ร่วมกันเป็นการโจมตีที่เรียกว่า "wp2shell" และ กรณีช่องโหว่ในผลิตภัณฑ์ VMware Avi Load Balancer หลายรายการ โดยมีรายละเอียดดังนี้

ผลิตภัณฑ์	รายละเอียดช่องโหว่	เวอร์ชั่นที่ได้รับผลกระทบ
WordPress	1. **ช่องโหว่ CVE-2026-63030** เป็นช่องโหว่ประเภท REST API Batch Endpoint Route Confusion โดยเป็นข้อผิดพลาดในการจับคู่เส้นทางกับตัวจัดการคำขอ โดยผู้ไม่หวังดีอาจส่งคำขอ HTTP ผ่านเส้นทาง /wp-json/batch/v1 เพื่อข้ามข้อกำหนดของ REST API เพื่อใช้ประโยชน์ร่วมกับช่องโหว่ CVE-2026-60137 2. **ช่องโหว่ CVE-2026-60137** เป็นช่องโหว่ประเภท SQL Injection ใน WP_Query ผ่านพารามิเตอร์ author_not_in ทำให้ข้อมูลที่ไม่ได้รับการตรวจสอบอย่างเพียงพอถูกนำไปประกอบเป็นคำสั่ง SQL และสั่งให้ระบบฐานข้อมูลประมวลผลคำสั่งที่ผู้ไม่หวังดีกำหนด ทำให้เข้าถึงและดึงข้อมูลที่มีความสำคัญออกจากฐานข้อมูล WordPress เช่น ข้อมูลบัญชีผู้ใช้งาน ค่าแฮชรหัสผ่าน และข้อมูลการตั้งค่าของเว็บไซต์ เป็นต้น รวมถึงการนำช่องโหว่นี้ไปใช้ร่วมกับ CVE-2026-63030 เพื่อรันคำสั่งบนเซิร์ฟเวอร์ การโจมตีสามารถเกิดได้กับ WordPress (Default Installation) โดยไม่จำเป็นต้องมีปลั๊กอินเพิ่มเติม และผู้ไม่หวังดีไม่จำเป็นต้องมีบัญชีผู้ใช้ในระบบ และเมื่อผู้ไม่หวังดีใช้ช่องโหว่ทั้ง 2 รายการร่วมกันจะสามารถทำ SQL Injection และ รันคำสั่งหรือโค้ดอันตรายบนเซิร์ฟเวอร์ WordPress ส่งผลให้ผู้ไม่หวังดีอาจควบคุมเว็บไซต์ เข้าถึงข้อมูล ติดตั้งปลั๊กอินหรือ Web Shell ที่เป็นอันตราย แก้ไขเนื้อหาเว็บไซต์ หรือ ใช้เซิร์ฟเวอร์ที่ถูกโจมตีเป็นจุดเริ่มต้นในการโจมตีระบบอื่นภายในองค์กรได้	**ช่องโหว่ CVE-2026-63030** ■ WordPress 6.9.0 - 6.9.4 ■ WordPress 7.0.0 - 7.0.1 **ช่องโหว่ CVE-2026-60137** ■ WordPress 6.8.0 - 6.8.5 ■ WordPress 6.9.0 - 6.9.4 ■ WordPress 7.0.0 - 7.0.1 WordPress ได้เปิดใช้การอัปเดตความปลอดภัยแบบบังคับผ่านระบบอัปเดตอัตโนมัติสำหรับเว็บไซต์ที่ใช้เวอร์ชันที่ได้รับผลกระทบ อย่างไรก็ตาม ผู้ดูแลระบบควรตรวจสอบหมายเลขเวอร์ชันที่ใช้งานจริงด้วยตนเอง

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 23 ก.ค. 2569
2. https://www.bleepingcomputer.com/news/security/wordpress-core-wp2shell-rce-flaws-get-public-exploits-patch-now/?
3. https://thehackernews.com/2026/07/new-wp2shell-wordpress-core-flaw-lets.html?

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

WordPress และ VMware Avi Load Balancer ออก Security Patch เพื่อแก้ไขช่องโหว่หลายรายการ

วันที่แจ้งเตือน 23 กรกฎาคม 2569

ผลิตภัณฑ์	รายละเอียดช่องโหว่	เวอร์ชั่นที่ได้รับผลกระทบ
VMware Avi Load Balancer	1. **CVE-2026-47865** เป็นช่องโหว่ประเภท Authentication Bypass ผู้ไม่หวังดีอาจข้ามกลไกการยืนยันตัวตนและสามารถเชื่อมต่อกับระบบและเข้าถึง Avi Control Plane โดยไม่จำเป็นต้องมีบัญชีผู้ใช้งานหรืออาศัยการดำเนินการจากผู้ใช้งาน 2. **CVE-2026-47866** เป็นช่องโหว่ประเภท Authorization Bypass ผู้ไม่หวังดีที่สามารถเชื่อมต่อกับระบบผ่านเครือข่าย เพื่อเข้าถึง Avi Control Plane 3. **CVE-2026-47867** และ **CVE-2026-47869** เป็นช่องโหว่ประเภท Remote Code Execution ผู้ไม่หวังดีที่สามารถเชื่อมต่อกับระบบผ่านเครือข่ายและมีสิทธิระดับสูง เพื่อเข้าถึง Avi Control Plane และสั่งรันโค้ดได้ 4. **CVE-2026-47868** เป็นช่องโหว่ประเภท Local Privilege Escalation ผู้ไม่หวังดีที่มีสิทธิเข้าถึงระบบ อาจใช้ประโยชน์จากช่องโหว่เพื่อยกระดับสิทธิและสั่งรันโค้ดด้วยสิทธิระดับ root 5. **CVE-2026-47870** เป็นช่องโหว่ประเภท Privilege Escalation ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนและสามารถเชื่อมต่อกับระบบผ่านเครือข่าย เพื่อใช้ประโยชน์จากช่องโหว่เพื่อสั่งรันโค้ดได้ 6. **CVE-2026-47871** เป็นช่องโหว่ประเภท Directory Traversal ซึ่งเกิดจากการตรวจสอบเส้นทางไฟล์ที่ไม่เหมาะสม ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนและสามารถเชื่อมต่อกับระบบผ่านเครือข่ายเพื่อเข้าถึงหรือดำเนินการกับไฟล์และไดเรกทอรีนอกตำแหน่งที่ระบบกำหนดได้ ช่องโหว่ จำนวน 7 รายการ ในผลิตภัณฑ์ Vmware Avi Load Balancer เกิดจากกระบวนการยืนยันตัวตนที่ไม่เหมาะสม (Improper Authentication) และทำให้ผู้โจมตีสามารถข้ามกลไกการยืนยันตัวตน (Authentication Bypass) โดยไม่จำเป็นต้องมีบัญชีผู้ใช้งานหรือมีสิทธิในระบบเพื่อเข้าถึงส่วนควบคุมระบบหรือ Avi Control Plane	VMware Avi Load Balancer ■ Version 32.1.1 ■ Version 31.1.1 - 31.2.2 ■ Version 30.1.1 - 30.2.6 ■ Version 22.1.1 - 22.1.7 Broadcom แนะนำให้ปรับปรุง VMware Avi Load Balancer เป็นเป็นเวอร์ชันล่าสุดที่แนะนำ

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 23 ก.ค. 2569
2. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37926?