

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

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



PHP ออกแพตช์ฉุกเฉินแก้ไขช่องโหว่ PHP2Shell (CVE-2026-109618 และ CVE-2026-109619)

วันที่แจ้งเตือน 22 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า มีการเปิดเผยช่องโหว่ระดับวิกฤต PHP2Shell (CVE-2026-109618 และ CVE-2026-109619) ใน PHP Runtime ซึ่งเป็นซอฟต์แวร์พื้นฐานที่ถูกใช้งานอย่างแพร่หลายในการให้บริการเว็บไซต์และเว็บแอปพลิเคชัน มีรายละเอียดดังนี้

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
PHP Group	ช่องโหว่ CVE-2026-109618 เป็นช่องโหว่ประเภท Out-of-Memory State Corruption ที่เกี่ยวข้องกับการจัดการกรณีที่ระบบเกิดภาวะหน่วยความจำไม่เพียงพอ ส่งผลให้อาจเกิดการหยุดการประมวลผลในขณะที่ข้อมูลภายในของคำขอไม่สมบูรณ์ ผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ดังกล่าวโดยส่งคำขอที่ใช้หน่วยความจำจำนวนมากเพื่อกระตุ้นเงื่อนไขดังกล่าว ช่องโหว่ CVE-2026-109619 เป็นช่องโหว่ประเภท Use-After-Free / Stale Global State เกิดจากการจัดการข้อมูลค้างในหน่วยความจำไม่สมบูรณ์ ทำให้ Worker Process อาจนำข้อมูลจากคำขอก่อนหน้านี้ที่ควรถูกลบไปแล้วกลับมาใช้งานอีกครั้ง โดยผู้ไม่หวังดีสามารถใช้ประโยชน์จากสภาวะดังกล่าว ในการรันคำสั่งจากระยะไกล (Remote Code Execution: RCE) และยึดควบคุมเซิร์ฟเวอร์ได้ ช่องโหว่นี้ได้รับการยืนยันผลกระทบกับทั้ง Apache mod_php และ PHP-FPM ในสภาพแวดล้อมที่เข้าเงื่อนไขการโจมตี - PHP Group แนะนำให้ผู้ผลิตผลิตภัณฑ์ดังกล่าว อัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อ PHP - เวอร์ชันที่ต่ำกว่า 8.2.35 - เวอร์ชันที่ต่ำกว่า 8.3.36 - เวอร์ชันที่ต่ำกว่า 8.4.27 - เวอร์ชันที่ต่ำกว่า 8.5.12 ซอฟต์แวร์เวอร์ชันแก้ไข - เวอร์ชัน 8.2.35 - เวอร์ชัน 8.3.36 - เวอร์ชัน 8.4.27 - เวอร์ชัน 8.5.12

ข้อมูลอ้างอิง

- <https://www.php.net/archive/2026.php#2026-10-21-5>
- <https://nvd.nist.gov/vuln/detail/cve-2026-109618>
- <https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>
- <https://nvd.nist.gov/vuln/detail/cve-2026-109619>
- <https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
- <https://www.bleepingcomputer.com/news/security/php-warns-admins-of-two-critical-flaws-emergency-patches-coming-tomorrow/>

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

มัลแวร์ YuanKong RAT มุ่งโจมตีผู้ใช้ Android เพื่อขโมยข้อมูลสำคัญ

วันที่แจ้งเตือน 22 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า นักวิจัยด้านความมั่นคงปลอดภัยตรวจพบมัลแวร์ Android Remote Access Trojan (RAT) ชื่อ YuanKong ซึ่งสามารถเข้าควบคุมอุปกรณ์จากระยะไกล เพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่าน รหัส PIN สำหรับธุรกรรมทางการเงิน และติดตามกิจกรรมของผู้ใช้งานผ่านฟังก์ชัน Accessibility ของโทรศัพท์ Android โดยไม่จำเป็นต้องขอสิทธิเข้าถึง SMS รายชื่อผู้ติดต่อ หรือบันทึกการโทรเหมือนมัลแวร์ทั่วไป

มัลแวร์ดังกล่าว สามารถบันทึกข้อมูลที่ใช้ป้อนบนหน้าจอ จับภาพหน้าจอ อ่านการแจ้งเตือน เข้าถึงคลิปปอร์ต โอนถ่ายไฟล์ และสั่งการอุปกรณ์จากระยะไกลได้ พร้อมทั้งยังสามารถสร้างหน้าจอปลอม (Overlay) เลียนแบบแอปพลิเคชันทางการเงินหรือหน้าจอป้อนรหัส PIN เพื่อหลอกขโมยข้อมูลสำคัญของผู้ใช้งานได้โดยตรง นอกจากนี้ มัลแวร์สามารถใช้ประโยชน์จากฟังก์ชัน Wireless Debugging ของ Android เพื่อเชื่อมต่อกับ Android Debug Bridge (ADB) และเพิ่มความสามารถในการควบคุมอุปกรณ์ รวมถึงทำให้มัลแวร์คงอยู่ในระบบได้ยาวนานขึ้น

เพื่อป้องกันความเสี่ยงและผลกระทบที่อาจเกิดขึ้น องค์กรควรพิจารณาดำเนินการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรที่ใช้อุปกรณ์ Android อย่างต่อเนื่อง โดยเน้นการติดตั้งแอปพลิเคชันจาก Google Play Store หรือแหล่งที่เชื่อถือได้เท่านั้น หลีกเลี่ยงการติดตั้งไฟล์ APK จากเว็บไซต์หรือลิงก์ที่ไม่รู้จัก ตรวจสอบและจำกัดสิทธิ์การเข้าถึง Accessibility ให้เฉพาะแอปที่มีความจำเป็น รวมถึงปิดใช้งานฟังก์ชัน Wireless Debugging เมื่อไม่ได้ใช้งาน เพื่อลดความเสี่ยงจากมัลแวร์ที่อาศัยสิทธิ์ดังกล่าวในการเข้าควบคุมอุปกรณ์และขโมยข้อมูลสำคัญ

ข้อมูลอ้างอิง

- <https://cybersecuritynews.com/new-yuankong-android-rat/>
- <https://starlabs.sg/blog/2026/10-yuankong-rat-the-android-remote-control-service-that-stamps-its-operators-names-into-every-build/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ