แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แคมเปญโจมตี SourTrade และช่องโหว่ใน Linux Kernel (CVE-2026-64600)

วันที่แจ้งเตือน 5 สิงหาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีการโจมตีผ่านเว็บไซต์ปลอม (SourTrade Campaign) และช่องโหว่ใน Linux Kernel (CVE-2026-64600) โดยมีรายละเอียดดังนี้

1. แคมเปญโจมตี SourTrade มุ่งเป้าไปที่นักลงทุนและผู้ใช้งานสินทรัพย์ดิจิทัล ซึ่งผู้ไม่หวังดีใช้การเผยแพร่โฆษณาออนไลน์แฝงมัลแวร์ (Malvertising) และเว็บไซต์ปลอมที่สร้างขึ้นเลียนแบบแพลตฟอร์มด้านการลงทุนและสินทรัพย์ดิจิทัล เพื่อหลอกผู้ใช้งานดาวน์โหลดมัลแวร์และติดตั้งในเครื่องคอมพิวเตอร์ โดยมัลแวร์จะดักจับและขโมยข้อมูล เช่น ค่าคุกกี้ บันทึกการกดคีย์บอร์ด และจับภาพหน้าจอ เป็นต้น และส่งกลับไปยังผู้ไม่หวังดี อีกทั้งเว็บไซต์ปลอมยังสามารถเก็บข้อมูลเบราว์เซอร์ ตำแหน่งภูมิศาสตร์ และรูปแบบการใช้งานของผู้ใช้งาน เพื่อคัดเลือกเป้าหมายและหลีกเลี่ยงการตรวจจับของระบบรักษาความมั่นคงปลอดภัย

เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น จึงขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการตรวจสอบข้อมูลที่บ่งชี้การโจมตี (IoCs) บล็อกโดเมนที่เกี่ยวข้อง พร้อมทั้งตรวจสอบข้อมูล logs เพื่อค้นหาพฤติกรรมที่ผิดปกติ และสร้างความตระหนักรู้ให้ผู้ใช้งานดาวน์โหลดโปรแกรมจากเว็บไซต์ทางการเท่านั้น

2. ช่องโหว่ใน Linux Kernel CVE-2026-64600 ซึ่งเป็นช่องโหว่ประเภทการยกระดับสิทธิ (Local Privilege Escalate) ที่เกิดจากข้อผิดพลาดแบบ Race Condition ในการทำงานของฟังก์ชัน XFS Reflink และ Copy-on-Write (Cow) โดยผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ในการเขียนทับไฟล์สำคัญของระบบและยกระดับสิทธิเป็น Root ได้ หากระบบใช้ XFS Filesystem ที่เปิดใช้งาน reflink = 1 และไฟล์สำคัญอยู่บน Filesystem เดียวกับพื้นที่ที่ผู้ใช้ทั่วไปสามารถเขียนข้อมูลได้ ทั้งนี้การเปลี่ยนแปลงที่เกิดขึ้นอาจยังคงอยู่หลังการ reboot และตรวจพบได้ยากจาก Kernel log ส่งผลให้ผู้ไม่หวังดีสามารถคงสิทธิการเข้าถึง ขโมยข้อมูล หรือขยายการโจมตีไปยังระบบอื่นได้

เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น จึงขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการติดตั้ง Patch ที่ได้รับการแก้ไขแล้วตามที่ผู้ผลิตให้คำแนะนำ พร้อมทั้งตรวจสอบการใช้งาน XFS และการตั้งค่า reflink = 1 ให้ความสำคัญกับการอัปเดตระบบที่มีความเสี่ยงสูง และเฝ้าระวังการเปลี่ยนแปลงไฟล์สำคัญ รวมถึงพฤติกรรมที่อาจบ่งชี้ถึงการยกระดับสิทธิ์หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อป้องกันผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 4 สิงหาคม 2569
2. https://cybersecuritynews.com/sourtrade-malvertising-malware
3. https://nvd.nist.gov/vuln/detail/CVE-2026-64600
4. https://thehackernews.com/2026/07/nine-year-old-refluxfs-linux-flaw-gives.html