

แจ้งเตือนเพื่อเฝ้าระวังช่องโหว่ใน Linux Kernel

เพื่อยกระดับสิทธิในระบบ (Privilege Escalation)

วันที่แจ้งเตือน 22 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบนักวิจัยได้รายงานช่องโหว่ใน Linux Kernel จำนวน 4 รายการ ส่งผลให้ผู้ไม่หวังดีสามารถแก้ไขข้อมูลในหน่วยความจำของ Kernel และใช้เป็นช่องทางในการยึดครองระบบด้วยสิทธิระดับ Root ได้

การโจมตี	ผลกระทบ
- DirtyAH6 (CVE-2026-80844) - ในส่วนการทำงานของ IPv6/IPsec Authentication Header - TUNderflow (CVE-2026-81000) - ในส่วน TUN/TAP Virtual Network Device - PPPoEject (CVE-2026-68121) - ในส่วน PPP over Ethernet (PPPoE) - DiagSpill (CVE-2026-74469) - ในส่วน SCTP Diagnostic Interface	- ทำให้ระบบหยุดชะงักหรือไม่สามารถให้บริการได้ (Denial of Service) - ช่องโหว่ DirtyAH6 และ DiagSpill สามารถถูกกระตุ้นผ่านเครือข่ายได้ - ยังไม่พบรายงานการใช้ช่องโหว่ทั้ง 4 รายการในการโจมตีจริง (In-the-Wild Exploitation) อย่างไรก็ตาม การที่ Exploit Code ถูกเผยแพร่สู่สาธารณะแล้ว อาจส่งผลให้ผู้ไม่หวังดีสามารถนำไปใช้โจมตีระบบที่ยังไม่ได้รับการอัปเดตได้ในอนาคต
ข้อเสนอแนะในการลดความเสี่ยง : - ตรวจสอบและปรับปรุง Linux Kernel ให้เป็นรุ่นที่ได้รับการแก้ไขช่องโหว่แล้ว Linux Kernel รุ่นที่มีแพตช์ครบทั้ง 4 ช่องโหว่ ได้แก่ 5.10.270, 5.15.221, 6.1.188, 6.6.157, 6.12.109, 6.18.50 และ 7.2.4 - ติดตามประกาศด้านความมั่นคงปลอดภัยจากผู้ผลิตระบบปฏิบัติการที่ใช้งานอยู่ เช่น Ubuntu, Debian, Red Hat หรือ SUSE - กรณีที่ยังไม่สามารถติดตั้งแพตช์ได้ทันที ควรพิจารณาปิดการใช้งาน Unprivileged User Namespaces * เพื่อลดความเสี่ยง - พิจารณาปิดการใช้งานฟังก์ชัน AH6, TUN/TAP, PPPoE และ SCTP หากไม่มีความจำเป็นในการใช้งาน * Unprivileged User Namespaces คือ พีเจอร์ของเคอร์เนล (Kernel) ที่อนุญาตให้ผู้ใช้ทั่วไป (Non-root user) สามารถสร้างสภาพแวดล้อมจำลอง (Isolated environment) โดยที่ผู้ใช้สามารถจำลองตัวเองให้มีสิทธิเป็น root โดยไม่มีผลกระทบต่อสิทธิในระบบหลัก (Host system)	

ข้อมูลอ้างอิง

1.

<https://thehackernews.com/2026/09/public-exploits-released-for-four-linux.html>
2.

<https://heyitsas.im/posts/lpe-quartet/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

CISA แจ้งเตือนช่องโหว่ Linux Kernel 3 รายการ ที่ถูกใช้โจมตีจริง

วันที่แจ้งเตือน 22 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า หน่วยงาน CISA (Cybersecurity and Infrastructure Security Agency) ของสหรัฐอเมริกา ได้เพิ่มช่องโหว่ 3 รายการใน Known Exploited Vulnerabilities (KEV) Catalog หลังพบหลักฐานว่ากำลังถูกใช้โจมตีจริง (Active Exploitation) ในระบบ Linux Kernel แล้วดังนี้

ช่องโหว่	ผลกระทบ
CVE-2025-39682 - เป็นช่องโหว่ความซอมิตพลาตใน TLS receive path ทำให้ผู้ใช้ภายในระบบ สามารถอ่านข้อมูลจากหน่วยความจำ หรือทำให้ระบบหยุดให้บริการ (DoS) ได้ CVE-2026-53266 - เป็นช่องโหว่ประเภท Out-of-bounds write ใน ebttables SNAT ARP rewrite path อาจนำไปสู่ DoS หรือยกระดับสิทธิ (Local Privilege Escalation) CVE-2025-39964 - เป็นช่องโหว่ประเภท Race Condition ใน AF_ALG socket อาจทำให้ระบบล่ม หรือกระทบความถูกต้องของกระบวนการเข้ารหัสข้อมูล (Data Integrity)	- CISA ยืนยันว่าช่องโหว่ทั้ง 3 รายการถูกใช้โจมตีแล้วในสภาพแวดล้อมจริง (in the wild) - ขณะนี้ยังไม่มีข้อมูลสาธารณะว่าผู้โจมตีใช้ช่องโหว่เหล่านี้อย่างไร หรือใช้ต่อเนื่องกันเป็น Attack Chain หรือไม่ - Red Hat ระบุว่า มี Public Exploit สำหรับช่องโหว่เหล่านี้และจัดว่าเป็นความเสี่ยงสูง ต้องเร่งแก้ไขโดยด่วน
คำแนะนำจาก CISA ในการลดความเสี่ยง : บริษัทควรเร่งตรวจสอบ Linux Server, Container Host และ Appliance ที่ใช้ Linux Kernel เวอร์ชันได้รับผลกระทบ และพิจารณาดำเนินการ Patch โดยเร็วที่สุด (ดูข้อมูลเพิ่มเติมจากอ้างอิง 2 - 4)	

ข้อมูลอ้างอิง

1. <https://thehackernews.com/2026/09/cisa-flags-three-linux-kernel.html>

2. <https://access.redhat.com/security/cve/cve-2025-39682>

3. <https://access.redhat.com/security/cve/cve-2026-53266>

4. <https://access.redhat.com/security/cve/cve-2025-39964>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT

Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์