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

Linux ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 10 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Linux ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ ได้แก่

ผู้ผลิต/ระบบ	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Linux	• **ช่องโหว่ CVE-2026-43499** ใน Linux Kernel เป็นช่องโหว่ประเภท Local Privilege Escalation (LPE) ซึ่งมีอยู่ในระบบมาตั้งแต่ปี 2011 เกิดจากความผิดพลาดในการจัดการหน่วยความจำของ Kernel (Uses-After-Free) เป็นผลให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ์เป็น root ได้ และหลบการกักกันของ Container เพื่อเข้าควบคุมระบบปฏิบัติการหลักหรือระบบอื่นขององค์กรได้ • Linux Distribution แนะนำให้อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้	ส่งผลกระทบต่อ Linux หลาย distribution เช่น SUSE, Ubuntu, RedHat เป็นต้น
	• **ช่องโหว่ CVE-2026-46242** ใน Linux Kernel เป็นช่องโหว่ประเภท Race Condition ร่วมกับ Uses-After-Free ใน Event Poll subsystem (epoll) ทำให้ผู้ไม่หวังดีที่ใช้สิทธิผู้ใช้งานทั่วไปสามารถยกระดับสิทธิเป็น Root ทั้งบนระบบปฏิบัติการ Linux และอุปกรณ์ Android เข้าควบคุมระบบและดำเนินการโจมตีเพิ่มเติมได้ • Linux Distribution แนะนำให้อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้	ส่งผลกระทบต่อ Linux Kernel เวอร์ชัน 6.4 หรือใหม่กว่า รวมถึงอุปกรณ์ Android ที่ใช้ Kernel เวอร์ชันดังกล่าว

ข้อมูลอ้างอิง CVE-2026-43499

1. https://nvd.nist.gov/vuln/detail/CVE-2026-43499
2. https://nebusec.ai/research/ionstack-part-2/
3. https://thehackernews.com/2026/07/15-year-old-ghostlock-flaw-enables-root.html

ข้อมูลอ้างอิง CVE-2026-466242

1. https://nvd.nist.gov/vuln/detail/CVE-2026-46242
2. https://github.com/J-jaeyoung/bad-epoll
3. https://securityaffairs.com/194795/hacking/bad-epoll-flaw-gives-attackers-root-access-on-linux-and-android.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

Linux ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 10 กรกฎาคม 2569

ผู้ผลิต/ระบบ	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Linux	• ช่องโหว่ **CVE-2026-53359** ใน Linux Kernel เป็นช่องโหว่ประเภท Use-After-Free ในกลไก Shadow MMU ของ Kernel-based Virtual Machine ทำให้ผู้ไม่หวังดียึดสิทธิ Root ใน Guest Virtual Machine แล้วหลบหลีกการตรวจจับด้านความมั่นคงปลอดภัย เพื่อเข้าควบคุม Guest Virtual Machine อื่นที่อยู่บน Host เดียวกันได้ • Linux Distribution แนะนำให้อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้	ส่งผลกระทบต่อผลิตภัณฑ์ KVM/x86 (Kernel-based Virtual Machine)

ข้อมูลอ้างอิง CVE-2026-53359

1. https://nvd.nist.gov/vuln/detail/CVE-2026-53359
2. https://github.com/V4bel/Januscape/blob/main/assets/write-up.md
3. https://www.bleepingcomputer.com/news/linux/new-januscape-linux-kernel-flaw-allows-vm-escape-on-intel-amd-devices/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ