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

Microsoft และ Linux ออก Security Patch เพื่อแก้ไขช่องโหว่ CVE-2026-42897 และ CVE-2026-46333

วันที่แจ้งเตือน 18 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

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

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	ช่องโหว่ CVE-2026-42897 เป็นช่องโหว่ประเภท Cross-Site Scripting (XSS) เกิดจากการตรวจสอบและจัดการข้อมูลนำเข้า ภายในระบบ OWA ที่ไม่ถูกต้องซึ่งถูกนำไปใช้โจมตี ทำให้ผู้ไม่หวังดีสามารถสร้างอีเมลที่มี JavaScript หรือ Payload อันตรายฝังอยู่ภายในและส่งไปยังผู้ใช้งาน Exchange Server เพื่อควบคุมระบบการต่าง ๆ ในนามของผู้ใช้งานได้โดยไม่ต้องรู้รหัสผ่าน	Microsoft Exchange Server แบบ On-Premises ที่เปิดใช้งาน Outlook Web Access (OWA) โดยเฉพาะ Exchange Server 2016, Exchange Server 2019 และ Exchange Server Subscription Edition ที่เปิดให้เข้าถึงผ่านอินเทอร์เน็ต
Linux	ช่องโหว่ CVE-2026-46333 เป็นช่องโหว่ในส่วนจัดการ Process ของ Linux Kernel ซึ่งเปิดโอกาสให้ผู้ไม่หวังดีสามารถแทรกกระบวนการก่อนที่ Process จะสิ้นสุดทำให้สามารถอ่านไฟล์สำคัญที่ถูกจำกัดสิทธิ์ไว้ (เช่น ไฟล์รหัสผ่าน /etc/shadow หรือ SSH Private Keys) ได้	กระทบ Linux ในหลายดิสทริบิวชั่น เช่น Ubuntu, Debian, CentOS และ Raspberry Pi OS

ข้อมูลอ้างอิง Microsoft

1. https://techcommunity.microsoft.com/blog/exchange/addressing-exchange-server-may-2026-vulnerability-cve-2026-42897/4518498
2. https://thehackernews.com/2026/05/on-prem-microsoft-exchange-server-cve.html
3. https://nvd.nist.gov/vuln/detail/CVE-2026-42897

ข้อมูลอ้างอิง Linux

1. https://cybersecuritynews.com/linux-kernel-vulnerability-ssh-keysign-pwn/
2. https://nvd.nist.gov/vuln/detail/CVE-2026-46333
3. https://github.com/0xdeadbeefnetwork/ssh-keysign-pwn

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

ช่องโหว่ในผลิตภัณฑ์ Ollama ส่งผลกระทบต่อข้อมูลหน่วยความจำรั่วไหล

วันที่แจ้งเตือน 18 พฤษภาคม 2569

ThaiCERT สกมช. ได้ติดตามข่าวสารกรณีช่องโหว่ใน Ollama หรือที่ชื่อว่า Bleeding Llama อาจส่งผลกระทบต่ออินสแตนซ์ของ Ollama ที่เปิดให้เข้าถึงจากอินเทอร์เน็ตกว่า 300,000 รายการ โดย Ollama เป็นแพลตฟอร์มโอเพนซอร์ส สำหรับรัน Large Language Model (LLM) หรือโมเดลภาษา AI เช่น Llama, Mistral, Gemma และ Qwen บนเครื่องหรือเซิร์ฟเวอร์ของผู้ใช้งานเอง แทนการเรียกใช้งานผ่านบริการ Cloud และช่องโหว่นี้อาจทำให้ข้อมูลสำคัญที่อยู่ในหน่วยความจำของระบบรั่วไหลได้

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
OLLAMA	ช่องโหว่ CVE-2026-7482 (CVSS V3.1 : 9.1) เป็นช่องโหว่ประเภท Heap Out-of-Bounds Read ในส่วน GGUF model loader ของ Ollama โดยเกิดจากการประมวลผลไฟล์โมเดล GGUF ที่มีค่าขนาดหรือ offset ของ tensor ไม่สอดคล้องกับขนาดไฟล์จริง ทำให้ระบบอ่านข้อมูลเกินขอบเขตหน่วยความจำ heap ระหว่างขั้นตอน quantization ทำให้ผู้ไม่หวังดีสามารถส่งไฟล์ GGUF ที่สร้างขึ้นไปยัง Ollama server ที่เปิดให้เข้าถึงผ่านเครือข่าย ส่งผลให้ข้อมูลในหน่วยความจำของ process อาจรั่วไหลได้ เช่น ข้อความ prompt, system prompt, ข้อมูลสนทนาของผู้ใช้อื่น, environment variables, API keys, tokens และ secrets ต่าง ๆ เป็นต้น	Ollama เวอร์ชันก่อน 0.17.1 

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 16 พ.ค. 2569
2. https://thehackernews.com/2026/05/ollama-out-of-bounds-read-vulnerability.html?
3. https://www.cyera.com/research/bleeding-llama-critical-unauthenticated-memory-leak-in-ollama?
4. https://www.cve.org/CVERecord?id=CVE-2026-7482