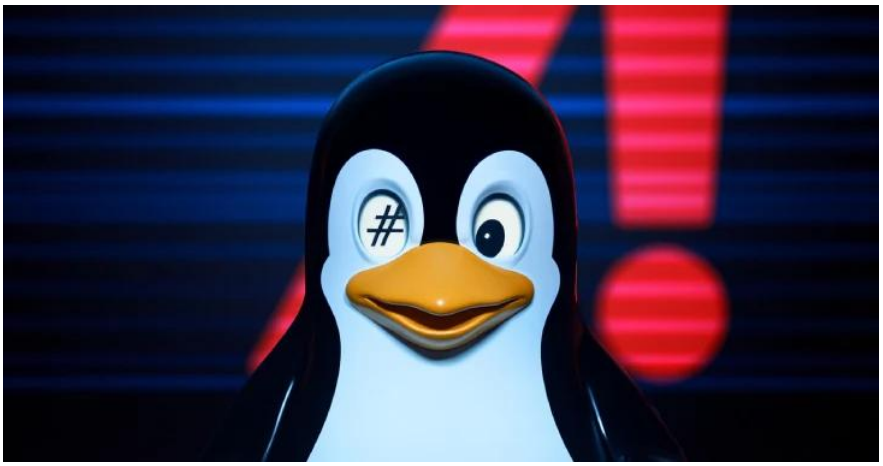
วันที่ 1 ตุลาคม 2568

CISA ส่งสัญญาณเตือนถึงช่องโหว่ร้ายแรงของ Sudo ที่ถูกใช้ประโยชน์ในระบบ Linux และ Unix



หน่วยงานความมั่นคงทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้ออกมาเตือนเมื่อวันจันทร์ที่ผ่านมาเกี่ยวกับช่องโหว่ร้ายแรงที่พบใน Sudo ซึ่งเป็นโปรแกรมบรรทัดคำสั่งที่ใช้กันอย่างแพร่หลายในระบบปฏิบัติการ Linux และ Unix โดยช่องโหว่นี้ถูกเพิ่มเข้าไปในรายการ Known Exploited Vulnerabilities (KEV) หลังมีหลักฐานยืนยันว่ากำลังถูกนำไปใช้โจมตีจริงแล้ว

ช่องโหว่ Sudo: รันคำสั่งในสิทธิ์ Root ได้แม้ไม่ได้รับอนุญาต

ช่องโหว่ของ Sudo ถูกระบุว่า CVE-2025-32463 (มีคะแนนความรุนแรง CVSS 9.3) ส่งผลกระทบต่อ Sudo เวอร์ชันก่อน 1.9.17p1 โดยถูกเปิดเผยครั้งแรกเมื่อเดือนกรกฎาคม 2025 โดยนักวิจัย Rich Mirch จาก Stratascale

รายละเอียดทางเทคนิค:

- CISA ระบุว่าช่องโหว่นี้เกี่ยวข้องกับการดึงการทำงานบางอย่างมาจากแหล่งที่ไม่น่าเชื่อถือ (untrusted configuration fetching)
- อนุญาตให้ผู้โจมตีที่อยู่ในระบบอยู่แล้ว (local attacker) สามารถใช้ตัวเลือก -R (--chroot) ของ sudo เพื่อรันคำสั่งใดๆ ในสิทธิ์ของ root ได้ อย่างสมบูรณ์ แม้ว่าสิทธิ์ดังกล่าวจะไม่ได้รับอนุญาตในไฟล์กำหนดค่า sudoers ก็ตาม

ขณะนี้ยังไม่ทราบแน่ชัดว่าช่องโหว่นี้ถูกโจมตีในลักษณะใด และใครเป็นผู้ที่อยู่เบื้องหลัง แต่การถูกเพิ่มเข้าในบัญชี KEV บ่งชี้ว่าภัยคุกคามนี้เป็นของจริง

CISA เพิ่มช่องโหว่ที่ถูกโจมตีจริงอีก 4 รายการในบัญชี KEV

นอกจากช่องโหว่ Sudo แล้ว CISA ยังได้เพิ่มช่องโหว่อีก 4 รายการที่มีการโจมตีจริงเข้าสู่บัญชี KEV โดยทั้งหมดนี้ถูกแนะนำให้หน่วยงานรัฐบาลกลาง (FCEB) เร่งดำเนินการแก้ไขภายในวันที่ 20 ตุลาคม 2025

ช่องโหว่และรายละเอียดเชิงเทคนิคมีดังนี้:

- **CVE-2021-21311 (Adminer):**
  - ผู้ถูกกระทบหลัก: Adminer
  - รายละเอียด: ช่องโหว่ Server-Side Request Forgery ที่เมื่อถูกใช้โจมตีอาจทำให้ผู้ไม่หวังดีเข้าถึงข้อมูลสำคัญได้ (Google Mandiant เปิดเผยเมื่อพฤษภาคม 2022 ว่ากลุ่ม UNC2903 ใช้โจมตี AWS IMDS)
- **CVE-2025-20352 (Cisco IOS/IOS XE):**
  - ผู้ถูกกระทบหลัก: Cisco IOS และ IOS XE
  - รายละเอียด: ช่องโหว่ Buffer Overflow บริเวณระบบ SNMP ซึ่งอาจทำให้เกิดการปฏิเสธการให้บริการ (DoS) หรือรันโค้ดอันตรายจากระยะไกลได้ (Cisco เปิดเผยเมื่อสัปดาห์ที่แล้วว่ามีการโจมตีจริงแล้ว)
- **CVE-2025-10035 (Fortra GoAnywhere MFT):**
  - ผู้ถูกกระทบหลัก: Fortra GoAnywhere MFT
  - รายละเอียด: ช่องโหว่ Deserialization of Untrusted Data ที่ผู้โจมตีใช้ลายเซ็นใบอนุญาตปลอมเพื่อทำให้ระบบโหลดวัตถุที่ควบคุมได้ และนำไปสู่การรันคำสั่งอันตราย (watchTowr Labs เปิดเผยเมื่อสัปดาห์ที่แล้วว่ามีการโจมตีจริงแล้ว)
- **CVE-2025-59689 (Libraesva ESG):**
  - ผู้ถูกกระทบหลัก: Libraesva Email Security Gateway (ESG)
  - รายละเอียด: ช่องโหว่ Command Injection ที่เปิดช่องให้ผู้โจมตีส่งคำสั่งผ่านไฟล์แนบอีเมลที่ถูกบีบอัด (Libraesva เปิดเผยเมื่อสัปดาห์ที่แล้วว่ามีการโจมตีจริงแล้ว)

ผู้ดูแลระบบที่ใช้ซอฟต์แวร์ข้างต้น โดยเฉพาะอย่างยิ่ง Linux/Unix ที่ใช้ Sudo ควรเร่งดำเนินการอัปเดตเป็น Sudo เวอร์ชัน 1.9.17p1 ขึ้นไปโดยเร็วที่สุดเพื่อป้องกันเครือข่ายของตนเอง

ข้อมูลอ้างอิง

Sep 30, 2025, By Ravie Lakshmanan
https://thehackernews.com/2025/09/cisa-sounds-alarm-on-critical-sudo-flaw.html